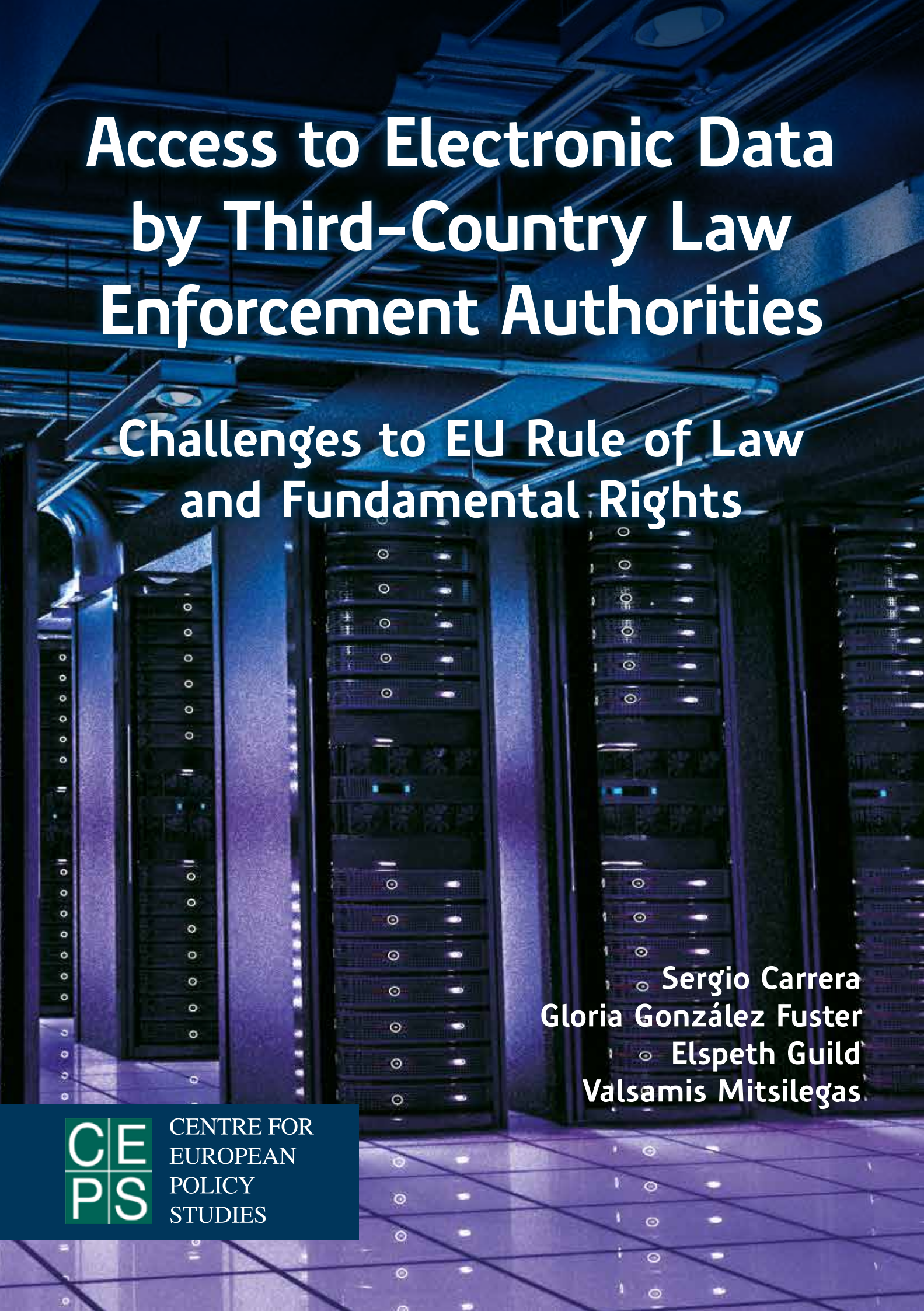


Access to Electronic Data by Third-Country Law Enforcement Authorities

Challenges to EU Rule of Law and Fundamental Rights

Sergio Carrera
Gloria González Fuster
Elspeth Guild
Valsamis Mitsilegas

CENTRE FOR EUROPEAN POLICY STUDIES

Access to Electronic Data by Third-Country Law Enforcement Authorities

Access to Electronic Data by Third-Country Law Enforcement Authorities

Challenges to EU Rule of Law and Fundamental Rights

Sergio Carrera
Gloria González Fuster
Elspeth Guild
Valsamis Mitsilegas

Centre for European Policy Studies (CEPS)
Brussels

The Centre for European Policy Studies (CEPS) is an independent policy research institute in Brussels. Its mission is to produce sound policy research leading to constructive solutions to the challenges facing Europe. This study was coordinated by the Justice and Home Affairs research unit of CEPS.

This study has been conducted thanks to the financial support of Microsoft. The independent analysis and opinions expressed in the study are solely those of the authors. The views expressed are those of the authors in a personal capacity only and cannot be attributed to any institution with which they are associated.

ISBN 978-94-6138-468-3

Centre for European Policy Studies
Place du Congrès 1, B-1000 Brussels
Tel: (32.2) 229.39.11 Fax: (32.2) 219.41.51
E-mail: info@ceps.eu
Internet: www.ceps.eu

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This study examines the challenges posed to European law by third-country access to data held by private companies for the purposes of law enforcement. It pays particular attention to the implications for rule of law and fundamental rights of foreign authorities' direct access to electronic information falling outside pre-established channels of supranational cooperation. A special focus is given to EU-US relations and the practical issues emerging in transatlantic relations covering mutual legal assistance and evidence gathering for law enforcement purposes in criminal proceedings.

Mutual Legal Assistance (MLA) treaties constitute the classical instrument allowing for foreign law-enforcement cooperation and assistance in the gathering of evidence in ongoing criminal investigations. A case in point is the EU-US MLA Agreement concluded in 2003. The proliferation and increasing uses of electronic communications has led to the emergence of law enforcement practices and voices attempting to have access outside MLA channels of cooperation to data controlled by private companies falling under EU jurisdiction.

The study assesses the main difficulties posed by unmediated third-country access from the perspective of European law. It argues that foreign access to data falling outside existing MLA processes only increases legal uncertainty and mistrust in transatlantic and private sector-public authorities' relations, as well as the public at large.

The analysis provides a detailed survey of the main EU legal instruments with direct relevance when assessing the lawfulness and legitimacy of access to data for law enforcement purposes. The EU exercises extensive legal competence over domains related to privacy, criminal justice and cybercrime, and has developed a large body of law providing common supranational rule-of-law standards applicable to a large majority of Member States.

The study then moves into an assessment of the main challenges posed by unmediated third-country access to electronic data against these EU legal standards. Third-country access to data outside established legal channels of mediated assistance (MLA) poses four legal and rule-of-law challenges:

First, ***the jurisdiction challenge*****:** An inherent tension exists between unmediated third-country access to data and the state-based territorial concept of jurisdiction. In criminal justice systems, the notion of jurisdiction requires the conclusion of MLAs to handle conflicts of law. Third-country access to data unlawfully bypasses existing legally-binding channels, resulting in legal insecurity and mistrust. The European concept of jurisdiction in the field of human rights differs also from that in the US. For all EU Member States the final word on their legal obligations is not in their

constitutions. They must comply with the European Convention on Human Rights (ECHR) and the supranational set of rule of law and fundamental rights provisions in the EU legal system.

Second, ***the lawfulness and 'forum-shopping' challenge*****:** These practices and current discussions in international and regional fora fail to pass the lawfulness test in EU law. Some security actors are using regional venues ('forum shopping') to agree on new rules that would put at risk EU rule-of-law standards by legalising unilateral law-enforcement access by third countries to data held by private-sector actors.

Discussions such as those in the Council of Europe (CoE) on cybercrime and transborder access to electronic data open serious questions from the perspective of EU law. The US and EU Member States are clearly committed to the rules laid down in the MLA agreement. EU Member States are now also committed to the system of access to evidence in criminal proceedings provided by instruments such as the so-called 'European Investigation Order' (EIO), which also limit their competences in foreign affairs in these matters. The external action of the EU and of Member States must be therefore consistent and compatible with this framework. Member States' commitments in the Council of Europe context must also be compatible with EU law.

Third, ***the challenge of alleged inefficiency*****:** Arguments alleging that MLA agreement models are inefficient are not substantiated by the available evidence or statistics on their uses and practical operability. While there exist certain obstacles affecting their practical implementation, this study argues that they can be overcome through a combined approach focused on bilateral case consultations, day-to-day contacts, stronger political commitments, more effective use of existing tools and sound financial, technological and human resources investments in their implementation.

Fourth, ***the privacy and data protection challenge*****:** Third-country access to data outside MLA agreements is contrary to EU data protection *acquis*. There are major dissimilarities between the EU and the US as regards data protection, not least the lack of effective judicial protection provided to EU citizens in US territory for privacy violations. This makes it difficult for EU institutions and Member States to ensure the safeguarding of EU fundamental rights and the benchmarks developed by the Luxembourg Court of Justice of the European Union in the 2014 *Digital Rights Ireland* ruling in transatlantic operating frameworks of cooperation in the domains of law enforcement and criminal justice.

Any future steps and developments should be therefore be closely tied to the rule of law and mediated access to data models in the scope of MLA processes and in conformity with EU law instruments and standards. The study then outlines three scenarios or options and puts forward a set of policy recommendations aimed at ensuring the rule of law and trust-based ways of moving forward on these issues. These are summarised below.

OPTION 1: *Enhancing the MLA Agreement Model*. This option would focus on ways to enhance existing legal provisions and procedures envisaged in the EU-US MLA framework within the current framework and without needing any general or specific legislative reform. Under this scenario the following specific policy recommendations are put forward:

- The EU should devise an independent evaluation/tracking system on the operability of the EU-US MLA Agreement. This should include statistical coverage of quantitative uses of MLA requests under the agreement. An EU-US Guide for Practitioners on the Use and Procedures within the EU-US MLA Agreement should be adopted. The Guide would provide 'promising practices' to relevant national authorities for overcoming practical obstacles and ensuring some streamlining of procedures.
- Eurojust could further facilitate cooperation between EU Member States and the US authorities in the execution of MLA requests, under close democratic and judicial scrutiny and that of relevant EU data protection bodies.
- Issues related to data protection, criminal justice and cybercrime now fall under EU competence. Any international negotiations covering these matters fall under exclusive EU external competence. The Commission is now in the driver's seat together with the European Parliament. The Commission and Parliament should also express concerns and centralise any further discussion on the EU's position regarding transborder access to data in the Council of Europe Cybercrime Committee.
- Key pre-conditions for further transatlantic cooperation should be the conclusion of the EU-US umbrella data protection agreement, the grading of EU citizens' effective judicial protection in the US and a swift EU inter-institutional consensus on the new data protection package.

OPTION 2: ***Improving the MLA Agreement Model.*** Under this scenario the EU-US MLA Agreement would be revised through legislative reform. The latter would be centred on bringing the agreement frameworks more in line with the EU-post Lisbon Treaty setting of legal norms and standards.

A starting point on such a potential revision should be the benchmarks laid down in the EU Directive on a European Investigation Order (EIO). These benchmarks provide clear safeguards on the basis of domestic and constitutional provisions in the executing and issuing Member State, proportionality test and fundamental rights exceptions, in addition to the judicialisation of MLA. Any legislative reform should not result in lowering existing rule-of-law standards and guarantees. The following recommendations are suggested under this option:

- The EU-US MLA model could be revised and amended in light of the EU post-Lisbon Treaty framework of legal standards and benchmarks in the domains of criminal justice and data protection. The EIO could be used as the minimum criteria or red lines for any future revision of the EU-US MLA framework. Eurojust should not become here a 'mediator' allowing for a model of hybrid access to electronic data.
- The EU should call for the consolidation and codification of existing EU rules and instruments dealing with judicial cooperation in criminal matters. This could lead to the adoption of a Common Corpus of European Criminal Law.

OPTION 3: ***Towards a Transatlantic Investigation Order.*** A third and long-term potential scenario would be the development of a common justice area across the Atlantic. Under this scenario, a recommendation is made to explore the future adoption of a Transatlantic Investigation Order (TIO) system which would speed and make more efficient judicial cooperation between the US and the EU. Such a system should start from rebuilding mutual trust on safeguarding rule of law and fundamental rights in US-EU security cooperation.

SECTION 1. INTRODUCTION

Third-country law enforcement access to electronic data is an issue of increasing relevance and concern in the European Union (EU). Unilateral access by foreign law enforcement authorities to individuals' data held by private companies creates a number of dilemmas and legal uncertainties when falling outside existing legal channels of transnational judicial cooperation.

The background of these issues is marked both by the large scale in the profusion of data about individuals produced and processed by private companies, and by the disruption of trust in transatlantic relations heralded by the Snowden revelations on large-scale electronic surveillance by the US.

The 2013 'Snowden revelations' brought to public attention the massive quantities of data and electronic communications that are constantly collected and generated by the most common of daily activities of citizens, and the fact that these could potentially be reached and accessed by authorities from a third country. Among the uncovered practices of large-scale mass surveillance supported by US authorities, a number of surveillance programmes stood out, such as PRISM, a programme allowing the US National Security Agency (NSA) to collect data about electronic communications from major companies operating globally.[1]

This study does not directly cover questions related to secret security-related large-scale surveillance, national security and intelligence communities' activities or practices. It focuses on **the legal issues and rule-of-law challenges raised by foreign authorities' access to electronic data for law enforcement purposes** in questions related to mutual legal assistance and evidence gathering in criminal proceedings.

The study assesses the implications of US authorities' access to electronic data under EU jurisdiction on privacy, the rights of the defence in criminal proceedings and more generally the rule of law in European Union law. Since the entry into force of the Lisbon Treaty five years ago, the EU has been recognised as having shared competence and has developed a solid body of Union law covering data protection, criminal justice and police/law enforcement cooperation and cybercrime. These provide **common European rules and normative standards** of particular relevance when assessing the challenges posed by unmediated access by foreign authorities of data held by private sector under the EU's jurisdiction.

[1] For an in-depth study on the challenges raised by large-scale electronic surveillance programmes to democratic rule of law refer to D. Bigo et al. (2013), "Mass Surveillance of Personal Data by EU Member States and its compatibility with EU Law", CEPS Liberty and Security in Europe Series, Centre for European Policy Studies, Brussels.

Among these standards stand chiefly the fundamental human rights of privacy and data protection, enshrined in Articles 7 and 8 of the EU Charter of Fundamental Rights. The evolving EU data protection *acquis* places the consent of the data subject[2] to access or disclosure of her/his personal data as one of the cornerstones of EU data protection law. 'Consent' constitutes a key ground for the legitimacy and lawfulness of states' interference with the fundamental human right of privacy. In a law enforcement and criminal justice context, this 'consent' assumes different shapes and translates into the mediation of an independent authority or court of law to allow for access and processing of individuals' data.

Transatlantic law enforcement access to data poses several dilemmas from an EU law viewpoint. There are important discrepancies between the EU and US legal systems in relation to personal data protection, but also as regards criminal law traditions and procedures. A key source of disagreement between the US and the EU when assessing the legality of access to data and interference with privacy relates to the question: **Who can give consent to access and share data?**

Any legal evaluation on whether US authorities can have access or request data directly from private companies does not find its answer in privacy or data protection law, but rather in **Mutual Legal Assistance (MLA) agreements**. Indeed, the differences in laws between the EU and US legal systems have been addressed through the conclusion of a MLA Agreement in 2003.

An MLA represents the classical treaty-based mechanism allowing for foreign law enforcement cooperation and assistance in ongoing criminal investigations and proceedings, while respecting the notions of jurisdiction and national sovereignty in criminal justice matters. It constitutes the most important legally-binding tool that provides the rules through which third-country authorities can lawfully issue requests for assistance in relation to the gathering of evidence from foreign jurisdictions.

Two basic steps apply in how MLAs operate, which are key at times of answering the question of 'who' can give consent to accessing electronic data: First, the receipt and assessment of the request for access will be delivered by a designated central authority of the requested state; and second, an independent judicial authority will validate or give consent to the legality for allowing access and processing of the data.

The proliferation and increasing use of electronic information has led to the emergence of voices calling for the fastening and legalisation of third-country access to data held by private companies outside MLA channels. A central argument used by those advocating for these practices is that the MLA model does not work effectively in practice, because of obstacles and barriers which make them too slow and burdensome.

Yet **bypassing existing legal channels of judicial and law enforcement cooperation would pose profound rule-of-law challenges**. The US and EU Member States are clearly committed to the

---

[2] Article 8 of the EU Charter of Fundamental Rights states, "[S]uch data must be processed fairly for specific purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law".

rules laid down in the MLA agreement. EU Member States are now also committed to the system of access to evidence in criminal proceedings provided by the so-called European Investigation Order (EIO), which limits their foreign affairs competences in these matters. The external action of the EU and of Member States must be therefore consistent and compatible with this framework. Member States' commitments in the Council of Europe context must also be compatible with EU law.

Moreover, claims alluding to the inefficiency of MLA procedures call for a cautious examination on the basis of existing evidence. Are these arguments based on objective data? What are the main current obstacles characterising the operability and implementation of MLA channels for mediated access to data in foreign jurisdictions, and what may be the actual issues behind them?

This study focuses on access to data held by private companies, and more specifically on transatlantic access to data held by companies providing their services in the EU and henceforth falling under European jurisdiction. These circumstances are of utmost relevance in practice. Data processed and held by companies has grown exponentially in recent decades, and the interest of law enforcement authorities in accessing it has increased proportionally.

Companies are facing increasing demands by governments and law enforcement authorities to have access to electronic individuals' data under their control. **These practices are blurring the 'rules of the game' and bring about legal uncertainty for private companies and all the relevant actors involved, which are often confronted with competing demands from different national governments authorities**. Companies are consequently confronted with increasing mistrust from individuals (and potential customers), courts and supranational institutions on the adequacy of privacy and due process in a context of large-scale pre-emptive surveillance.

This study aims at identifying and assessing the main issues and difficulties that the proliferation and potential legalisation of third-country access to data outside MLA channels triggers from the perspective EU law. It is argued that unmediated models of foreign authorities' access to electronic data controlled by private companies should be avoided as they pose profound fundamental challenges to fundamental rights and rule of law. EU law as it stands simply does not allow the direct interaction between US authorities (or any other third country for the same matter) and private companies.

While claims for speed and rapidity can be understood from a law-enforcement perspective, these may jeopardise the effective delivery of justice, rule of law and the proper safeguarding of privacy and the rights of defence. Remote access to data will only increase mistrust in transatlantic relations and private sector-public institution relations as well as by individuals.

The analysis has been structured into five main sections.[3] After this introductory section, Section 2 outlines the ways in which foreign authorities access to data can be framed by different models, and presents existing instruments relevant in a transatlantic context. Section 3 describes the applicable EU legal standards in a post-Lisbon Treaty landscape. Section 4 identifies the key legal and rule-of-law challenges raised by non-MLA models of access to data advanced in section 2. Finally, Section 5 discusses possible upcoming steps or scenarios, and puts forward a set of recommendations to European institutions.

[3] The research presented has been based on an assessment of key legal and policy documents, as well as relevant literature. This has been combined with semi-structured interviews with key actors, practitioners and policy-makers. Interviews were conducted in Brussels, Washington, D.C., and The Hague during the spring and summer of 2015. Preliminary findings were discussed at a closed-doors expert meeting held in March 2015 at the Centre for European Policy Studies (CEPS), Brussels.

SECTION 2. MODELS OF THIRD-COUNTRY ACCESS TO DATA

KEY FINDINGS

- There are three main models of third-country access to data: first, mediated access schemes (corresponding with Mutual Legal Assistance agreements); second, unmediated access to data practices or remote access claims; and third, hybrid access to data models with a third party as non-judicially independent mediator. The two last models stand in a difficult relationship with the rule of law.
- The exact ways in which mediated access models work in practice often depends on the specific features characterising the country's domestic legal and judicial system (adversarial or non-adversarial). Under mediated models two moments are of importance: First, the receipt and assessment of the request for access by a designated central authority of the requested state; and second, the involvement of an independent judicial authority in validating access and processing of the data.
- For the purposes of EU law, 'competent national law enforcement authority' usually means the police authorities, yet important variations exist across EU Member States. This concept does not include intelligence services. A court for the purposes of EU law must be characterised by its independence, impartiality and focus on settling the rule of law, which all together enable delivering effective remedies.
- There is a fundamental difference between data or information, and evidence. For data to be considered "evidence" in criminal justice procedures, its access, processing and use in criminal proceedings will need to pass a legality test by an independent judicial authority.
- The EU has developed so-called 'hybrid models' of access to data through the involvement of EU agencies (e.g. Europol). These models lack a proper oversight system by an independent judicial authority. They are affected by accountability and transparency deficits.

Foreign authorities' access to data may take place in different ways and forms. This section presents **the three main models** of transnational access to data, and considers their current and potential relevance for the EU. These three basic different patterns or 'models' can be broadly identified, as described below.

First, data-accessing can occur in accordance with **mediated access schemes**, whereby an authority in the requesting state wishing to obtain access to data under the jurisdiction of another state contacts a designated central authority of that country with recognised competence to order access and data transfers from private companies (section 2.1 below). Access to data is supervised by the central authority and an independent court or tribunal of the requested country. This model corresponds to the system laid down in MLA agreements.

A second model relates to **unmediated access practices or remote third-country access systems**, whereby an authority in the requesting foreign country communicates its demands directly to the private company holding or controlling the data. This is so even if the company's decision to disclose the data can be considered to fall under another jurisdiction and access to the data would entail legal responsibility there (section 2.2). This model lacks consent by the requested state and any mediation by independent judicial authority.

A third possibility is a model requiring the authority of the requesting country to transmit its request not to an authority in the requested jurisdiction but which has an *ad hoc* authority, not corresponding with a specific state. This authority shall thus act as a special, *sui generis* and non-judicially independent 'mediator'. This kind of **'hybrid access to data' model** raises similar challenges due to the lack of judicial supervision and accountability of the decision allowing for access to information (section 2.3).

2.1. Mediated Access Model

Traditionally, EU Member States have privileged the model of mediated access to authorise the obtaining of data for law enforcement purposes in a transnational context or when cooperating with third countries. This paradigm is behind the adoption of Mutual Legal Assistance Treaties, and the most relevant example epitomising this approach in the EU is the EU-US Agreement on Mutual Legal Assistance (hereinafter EU-US MLA).

The EU-US MLA was signed in 2003, together with a parallel transatlantic agreement on extradition.[4] They were concluded in a complex legal landscape, predating the entry into force of the Lisbon Treaty, where the former EU Treaties did not confer expressly to the EU legal personality and where the Union still had limited competences over police and criminal justice cooperation affairs.[5] As a result, the entry into force of the EU-US MLA had to follow the exchange of instruments by the parties indicating

[4] Agreement on extradition between the European Union and the United States of America, OJ L181, 19 July 2003, p. 27; Agreement on mutual legal assistance between the European Union and the United States of America, OJ L181, 19 July 2003, p. 34. See also the Council Decision, on the basis of Articles 24 and 38 TEU, concerning the signature of these agreements: OJ L181, 19 July 2003, p. 25.

[5] They were as a matter of fact the first international agreements negotiated by the EU under its 'Third Pillar'. For details, see: V. Mitsilegas (2003), "The New EU-US Co-operation on Extradition, Mutual Legal Assistance and the Exchange of Police Data", *European Foreign Affairs Review*, Vol. 8, pp. 515-536.

that they had completed their internal procedures for this purpose.[6] Domestic procedures were only completed in 2009,[7] and the agreements entered into force only on 1 February 2010.

Under this model **there are two decisive moments in the 'requested State' receiving an MLAT request**: The first corresponds to **the receipt of the request by the designated central authority**, which is in charge of examining the MLA request against existing domestic legal requirements and standards; and the second relates to **the transmission of that request from the central designated authority to the prosecutor's office to obtain a court order**. The issuing of a court order is required for the prosecutor to obtain the requested electronic data lawfully. Once issued, the data will be examined against the MLA request, and will then be transmitted to the requesting State via the designated MLA channels.

The ways in which the 'mediated access' model work in practice or the procedures for sending/receiving MLA requests may differ depending on the specific legal tradition of the country at hand. Differences may exist, for instance, when looking at adversarial and non-adversarial (often referred to also as 'inquisitorial') systems, which usually operate in civil law traditions. These traditions determine the exact ways and procedures through which criminal justice investigations and cases are to be conducted in different legal systems.[8] In adversarial systems such as the US, how the MLAT procedure works in practice has been described as follows:[9]

> Supervising the execution of incoming MLATs—requests for assistance from foreign jurisdictions—requires direct federal district court oversight and involvement. In contrast, the courts play no part in initiating or processing outgoing MLAT requests. That is the province of the executive branch. Requests from abroad ("incoming requests") for legal assistance are directed to a country's designated "central authority", usually the Department (or Ministry) of Justice. The central authority, in turn, transmits the MLAT or letter rogatory-related communication to the appropriate court or government entity. When a federal prosecutor appears before a U.S. district court requesting assistance on behalf of a foreign state or provides notice

---

[6] Article 22(1) of the Mutual Legal Assistance Agreement. This provision triggered Article 24(5) of the Treaty on European Union (TEU), allowing Member States to indicate that they need to follow internal constitutional procedures.

[7] Council Decision 2009/820/CFSP on the conclusion on behalf of the European Union of the Agreement on extradition between the European Union and the United States of America and the Agreement on mutual legal assistance between the European Union and the United States of America, OJ L291, 7.11.2009, p. 40.

[8] One of the main differences between the adversarial/common law and non-adversarial (inquisitorial) systems is the role of the judge. In adversarial/common law, the judge does not take up the role of investigating the case her/himself, but rather plays a role of neutral mediator between the prosecutor and the defence. The most persuasive and effective adversary convincing the judge will win the case. In a non-adversarial or inquisitorial system, the judge takes up an investigative role in examining the facts of a given case.

[9] See http://www.fjc.gov/public/pdf.nsf/lookup/mlat-lr-guide-funk-fjc-2014.pdf/$file/mlat-lr-guide-funk-fjc-2014.pdf.

> that the U.S. government will seek assistance from a foreign state, the prosecutor acts at the direction of the U.S. Department of Justice's Office of International Affairs (OIA). OIA is the United States' central authority and de facto functional hub for all outgoing and incoming requests for transnational investigation and litigation assistance.

Furthermore, it is important to be circumspect regarding the expression 'law enforcement access to data', as it may be deceiving when trying to understand mediated access models. The answer to **the question of 'who' is a 'competent law enforcement authority' remains by and large disputed**. It is generally intertwined with specific national legal traditions. This is in turn problematic from the perspective of legal certainty and safeguarding EU law standards when assessing the lawfulness of access to data for law enforcement and criminal justice purposes.

The EU is here not an exception. By and large, EU Member States have designated national **police authorities and services** 'competent national law enforcement authorities'. This corresponds with Article 2 of the Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union, which states that a "'competent law enforcement authority' [is] a national police, customs or other authority that is authorised by national law to detect, prevent and investigate offences or criminal activities and to exercise authority and take coercive measures in the context of such activities". However, **important variations exist in practice**.[10] Moreover, this provision emphasises that those agencies covering "national security issues", chiefly intelligence services, are not covered by this concept.

In the scope of EU criminal justice law, **the definition of 'judicial authority'** would come from the text of the Directive on the European Investigation Order (EIO) (see section 3.3 below for a detailed analysis).[11] The terms "court" or "tribunal" have not been provided in the Treaties. The Court of Justice of the European Union (CJEU) has held that the terms have **autonomous and self-standing meanings in the context of mutual**

[10] According to the Guidelines on the application of this Framework Decision published by the Council in 2009, the differentiation characterising the designation of authorities has been confirmed. A substantial majority of EU Member States have selected police authorities and services. That notwithstanding, four Member States have included prosecutors' offices (e.g. Czech Republic, Estonia, Latvia and Hungary). Others have designated military/defence authorities (e.g. Estonia, France, Latvia, Lithuania, Poland and Romania). Financial/Tax authorities have been designated in Germany, Estonia, Greece, Ireland, Latvia, Poland, Sweden and the UK. Several Member States have nominated border and customs authorities (e.g. Belgium, Czech Republic, Estonia, Latvia, Luxembourg, Romania, Sweden and the UK). Finally, in a few cases Member States have designated ministries or special directorates in ministries (e.g. Austria, Bulgaria, Italy, Latvia, Luxembourg or Romania). Council of the EU, Guidelines on the Implementation of Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union, 8083/09, 7 April 2009, Brussels.

[11] Directive 2014/41 regarding the European Investigation Order in Criminal Matters, OJ L 130, 1.5.2014.

recognition in criminal matters in EU law.[12] For a body to be considered a court with jurisdiction for the purposes of EU law a number of criteria need to be met. These include whether it applies the rule of law and is independent and impartial, with no other interest than applying the rule of law. [13] Therefore, for the purposes of this study, every time "law enforcement access" is used, reference is made to access to data by authorities unmediated access models, and which therefore lack independence from the executive of the country concerned or their interests are not impartial for applying the rule of law.

2.2. Unmediated Access Model

This model corresponds with access by third-country authorities to data falling under EU jurisdiction without going through the competent authority that could authorise the access in the relevant EU Member State under the MLA channels of cooperation. A key distinguishing feature of this model is **the lack of consent by the requested stated and the non-intervention by an independent authority** in the requested EU state validating the lawfulness of accessing and processing data. Foreign authorities' deliver a data request or legal order directly to private companies rather than using existing MLAT processes.

Under this model, a third country actually asserts the authority under its own national law to access electronic data falling under the scope of EU laws – data which might or might not be stored in EU territory, but which still remains under Union's jurisdiction. This scheme can generate multiple conflicts of law when, in spite of the requesting country's perception, the transfer of data would trigger legal consequences or liabilities in the affected country for the requested private company. As illustrated in section 4 of this study, **this model poses far-reaching legal and rule-of-law challenges from the perspective of EU law**.

---

[12] For more information on the principle of mutual recognition see http://ec.europa.eu/justice/criminal/recognition-decision/index_en.htm.

[13] Refer to P. Aalto et al. (2014), "Article 47 – Right to an Effective Remedy and to a Fair Trial", in S. Peers, T. Hervey, J. Kenner and A. Ward (eds), *The EU Charter of Fundamental Rights: A Commentary*, Oxford: Hart Publishing, p. 1208. See for instance Case C-54/96 Dorsch and Case C-506/04 Wilson of 19 September 2006. In the latter judgment the CJEU clarified that the notion of independence is a constitutive element of the act of adjudication and differentiated two main dimensions: first, that the body is free from external intervention or pressure; second, that it is impartial, with no other interest than applying the rule of law. See paragraph 51 of the judgment which states, "The first aspect, which is external, presumes that the body is protected against external intervention or pressure liable to jeopardise the independent judgment of its members as regards proceedings before them. That essential freedom from such external factors requires certain guarantees sufficient to protect the person of those who have the task of adjudicating in a dispute, such as guarantees against removal from office". And paragraph 52 which reads, "The second aspect, which is internal, is linked to impartiality and seeks to ensure a level playing field for the parties to the proceedings and their respective interests with regard to the subject-matter of those proceedings. That aspect requires objectivity and the absence of any interest in the outcome of the proceedings apart from the strict application of the rule of law."

The use of this model brings in sharp relief the need to distinguish between what is "data" and what constitutes "evidence" before a court of law. Unmediated access models highlight the distinction **between electronic data or e-information and "evidence" in criminal proceedings**. Data or information cannot always be considered accurate, reliable and lawful evidence.[14] While law enforcement may have access to large-scale data of individuals, some of which may be often qualified as "intelligence", this does not mean that this kind of information will pass the lawfulness test for it to be accepted as evidence before an independent judge in a pending criminal case. The study therefore avoids using notions such as 'electronic or cloud evidence', as they are misleading of the material scope of the debate.

Discussions in the context of the Council of Europe's Cybercrime Convention on transborder access to data without going through existing mutual legal assistance channels have hinted towards the possible inscription of this unmediated model in future instruments which would amend the Budapest Convention (section 2.2.1). Furthermore, a practical case where the validity of this model is at stake is currently pending in the US, the Microsoft Search Warrant case (section 2.2.2).

2.2.1. Council of Europe Cybercrime Convention Committee

Transnational law enforcement access to data has been the focus of particular attention in relation to the Council of Europe's work on cybercrime. In this context, the key legal instrument is the Convention on Cybercrime of 23 November 2001, also known as the 'Budapest Convention'.[15]

The Convention on Cybercrime was the first international treaty specifically devoted to cybercrime and to synchronising national laws on these matters. Developed in 2001, it came into force in 2004. The Convention encourages international cooperation in the investigation and prosecution of offenses such as illegal access and illegal interception of data and communications, data interference, system interference or misuse of devices. The Convention has not been ratified by all EU Member States.[16] The **Convention has nevertheless been signed and ratified by a number of countries that are not Member States of the Council of Europe**, including the US, Australia and Japan.

---

[14] K. Roach (2010), "The Eroding Distinction Between Intelligence and Evidence in Terrorism Investigations", in N. McGarrity, A. Lynch and G. Williams (eds), *Counter-Terrorism and Beyond*, London: Routledge, pp. 48-68. Roach argues, "[T]he creation of sweeping new terrorism offences after 9/11 has blurred the traditional distinctions between intelligence and evidence. Such new offences reflect an intelligence mind-set that focuses on threats, risk, associations and suspicion as opposed to an evidence or criminal law mind-set that focuses on acts, accomplices and guilt. One implication of the blurring of the distinction between intelligence and evidence is a convergence between the work of police forces and security intelligence agencies in terrorism investigations. This convergence is driven in part by the demands of prevention".

[15] Retrievable from http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm.

[16] Greece, Ireland, Latvia, Poland and Sweden have signed but not ratified it. Some Member States of the Council of Europe, such as Russia, have not signed it.

The Convention on Cybercrime includes a provision on "*trans-border access to stored computer data with consent or where publicly available"* in Article 32.b. In accordance with this Article, a party may

> without the authorisation of another Party, access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.

The provision tackles the issue of the possible access to data from a requesting country directly from a 'person' in the requested country without the authorisation of the latter, and hence outside existing MLA frameworks.

The Cybercrime Convention Committee (T-CY),[17] which aims at facilitating the effective use and implementation of the Convention, and particularly its Cloud Evidence Group, **has opened a process aiming at amending this Article**. The issue of transnational law enforcement access to data has also been given special relevance in the discussions of Cybercrime@Octopus, a Council of Europe project based on voluntary contributions aimed at assisting countries in implementation and strengthening data protection and rule-of-law safeguards.[18] In 2013, a suggestion was made at an Octopus Conference to address the matter of cross-border access to personal data between States' parties in a new Protocol or other binding international instrument.[19]

The main idea of such a new Protocol would be to allow or 'legalise' an unmediated model of access to data, where remote access or data requests issued directly to private companies would be permissible without going through existing cooperation or MLA channels. The justification put forward for a revision has been that the increasing use of electronic and cloud-based data has made the work of law enforcement authorities more difficult and that existing MLA arrangements are inefficient.

This initiative has created controversy in several EU instances in Brussels. **The European Parliament has expressed serious concerns** about the work carried out within the Council of Europe's Cybercrime Convention Committee with a view to developing an additional protocol on the

---

[17] See http://www.coe.int/en/web/cybercrime/tcy. See also the Guidance Note that it developed on the use of Article 32 at https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e726a.

[18] The project ensures the organisation of annual conferences, supports the Cybercrime Convention Committee, and provides advice and assistance to states parties. See http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Cybercrime@Octopus/Cybercrime@Octopus_en.asp.

[19] The environment surrounding this initiative has been described as "a situation where cross-border access to personal data by national law-enforcement agencies is becoming effectively unregulated and close to arbitrary". D. Korff (2014), "The Rule of Law on the Internet and in the Wider Digital World", Issue Paper Published by the Council of Europe Commissioner for Human Rights, Council of Europe.

interpretation of Article 32 of the Convention on Cybercrime.[20] As we will study in detail in section 4 below, the European Parliament has raised serious doubts related to questions of EU legal competence and compatibility of these regional debates with existing EU law standards.

2.2.2. The Microsoft Search Warrant Case

A case exemplifying the unmediated access model is currently pending before US courts, more concretely before the U.S. Court of Appeals for the Second Circuit.[21] It was initiated in 2013 as **US authorities sought access to data related to an email account held by the company Microsoft**.

In December 2013, the US government presented an affidavit establishing probable cause to believe that a Microsoft-based email account was being used for narcotics trafficking. The competent US magistrate judge issued a search warrant pursuant to the 1986 Stored Communications Act (SCA),[22] that is, an 'SCA warrant'. It requested Microsoft to disclose all the contents of the email account. Microsoft, however, refused to disclose the requested records on the basis that the US court could not compel Microsoft to do so because the data were stored in a data centre in Dublin (Ireland).

Microsoft then presented a motion before the judge to vacate the warrant, which was denied, as **the judge stressed the warrant obliged Microsoft to produce the solicited data regardless of the location**.[23] The judge took the position that the request by the government was not a conventional warrant, but rather a 'compelled disclosure' or subpoena, and held that in any case it was not an extraterritorial assertion of US law.

This ruling was challenged before the U.S. District Court for the Southern District of New York, but the District Court's Chief Judge confirmed the prior decision,[24] maintaining that the U.S. Congress had intended the SCA to compel electronic communications providers to produce any information under their control, including information stored abroad. The chief judge thus entered an Order against Microsoft for the continuing refusal to comply with the warrant, but the company was allowed to appeal to the Second Circuit.[25]

---

[20] European Parliament, Resolution of 10 December 2013 on unleashing the potential of cloud computing in Europe (2013/2063(INI)), Strasbourg, § 72.

[21] In "Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp.", 15 F. Supp. 3d 466 (S.D.N.Y. 2014).

[22] The SCA is part of the Electronic Communications Privacy Act (ECPA), Pub. L. No. 99-508, 100 Stat. 1848 (1986), and regulates law enforcement access to content communications when in the possession of a provider of an "electronic communications service" (ECS) or a "remote computing service" (RCS) to the public.

[23] "Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp.", 15 F Supp. 3d 466, 472 (S.D.N.Y 2014).

[24] In "Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp.", No 14-2985-CV, 2014 WL 4629624 (S.D.N.Y. 29 August 2014).

[25] Brief for Appellant at 2, Microsoft v. US, No. 14-2985-cv (2nd Cir. 2014).

Microsoft has contested the decision on the grounds that the records are stored in a data centre in foreign country, not owned by Microsoft but rather by the email user, and that the order entails a conflict of laws and the impermissible exercise of extraterritorial authority.[26] The US government has argued that there is no conflict of laws, and that the US retains the authority to order an entity within its jurisdiction to repatriate records.[27] From this viewpoint, as claimed by the US government, Microsoft being a US-based company, it would enjoy 'corporate citizenship' to which are attached some responsibilities, including the duty to comply with a disclosure order issued by a US court.[28]

An Amicus Curiae Brief presented by two Members of the European Parliament (MEPs)[29] in support of Microsoft argues that the company could be allowed to transfer the data through MLAT procedures, but not directly from Microsoft to US authorities.[30] Ireland also submitted an Amicus Curiae, observing foreign courts should respect Irish sovereignty,[31] and stating that it "would be pleased to consider, as expeditiously as possible, a request under the treaty, should one be made" under the Criminal Justice (Mutual Assistance) Act.[32]

An Amicus Brief presented by Digital Rights Ireland Limited (DRI), Liberty and the Open Rights Group[33] underlines that **the EU MLAT must be regarded as 'self-executing' in US law**, and thus to affect previous US law without requiring any further legislation. Stressing the mandatory need to follow the MLAT provisions, it notes that "[a]dopting the US position would allow the US government unilaterally to substitute US court compulsion for the balancing process represented by the MLAT information request procedures".[34]

The US government argues that using MLATs would not be effective, as the data could quickly be moved to a different country, and because mutual legal assistance procedures are lengthy and do not result in a prompt

---

[26] Microsoft has been joined by nine amici curiae comprising two Members of the European Parliament, technology and media companies, trade associations and civil society, and representatives from the academic community.

[27] In the view of the US government, "the power of compelled disclosure reaches records stored abroad so long as there is personal jurisdiction over the custodian and the custodian has control over the records". Case 14-2985, Document 212, 9 March 2015, p. 9.

[28] Ibid., p. 57.

[29] Jan Philipp Albrecht and Marju Lauristin.

[30] Amicus Curiae Albrecht, Document 148, 19 December 2014, p. 9.

[31] Brief of Amicus Curiae Ireland, Document 164, 23 December 2014, p. 3.

[32] Brief of Amicus Curiae Ireland, p. 4. The Act is available at http://www.irishstatutebook.ie/2008/en/act/pub/0007/index.html.

[33] Amicus Brief Digital Rights Ireland Limited, Liberty and the Open Rights Group, Document 101, 15 December 2014, pp. 18-20.

[34] Amicus Brief Digital Rights Ireland Limited, Liberty and the Open Rights Group, Document 101, 15 December 2014, p. 25.

disclosure of records.[35] The validity of this argument is contested in the DRI and others' Amicus Brief, advancing that mutual legal assistance between the US and Ireland is believed to function efficiently, and stressing that "European law does not block the disclosure of information to foreign law enforcement authorities so long as there are sufficient protections of individual rights within the mechanism for such disclosure".[36]

2.3. Hybrid Access Models

The two previously described access models do not exhaust all existing relevant scenarios or frameworks of access and exchange of data in EU-US relations. The EU has in some circumstances searched for **'alternative systems' to configure paths for granting access to data to law enforcement authorities across the Atlantic**. A case in point has been an EU-US Agreement on the exchange of financial information called the Terrorist Finance Tracking Program (TFTP).

In 2006 the media disclosed that for several years US authorities had been accessing massive amounts of personal data related to European financial transactions by obtaining the information directly from a private company, the Society for Worldwide Interbank Financial Telecommunication (SWIFT), based in Belgium.[37] The situation was addressed with the signature of an EU-US agreement under which the EU allows for the transfer of European financial data for its use in the context of the U.S. Terrorist Finance Tracking Program (TFTP). After the European Parliament gave its consent to the agreement, the agreement between the EU and the US on the processing and transfer of Financial Messaging Data from the EU to the US for the purposes of the TFTP came into force in August 2010.[38]

The TFTP allows for the transfer to the U.S. Treasury Department of data stored in the territory of the EU for the purpose of the prevention, investigation, detection, or prosecution of terrorism or terrorist financing. The Agreement grants a special role to the EU's law enforcement agency, Europol (The European Police Office) in The Hague. **Europol is responsible for verifying that the requests emanating from the US meet the requirements described in the Agreement**. This includes notably terms of clearly identifying the requested data, substantiating their necessity, and being as narrow as possible.[39] Once this verification has taken place, the data request also becomes legally binding under EU law.

---

[35] Case 14-2985, Document 212, pp. 51-52.

[36] Amicus Brief Digital Rights Ireland Limited, Liberty and the Open Rights Group, Document 101, 12.15.2014, pp. 13-14.

[37] See G. González Fuster, P. De Hert and S. Gutwirth (2008), "SWIFT and the vulnerability of transatlantic data transfers", *International Review of Law, Computers & Technology*, Vol. 22, No. 1, pp. 191-202. See also A. Amicelle (2011), "The Great (Data) Bank Robbery: Terrorist Finance Tracking Program and the 'SWIFT Affair'", Research Question 36, CERI, Sciences-Po, Paris.

[38] OJ L 195/5 of 27.7.2010.

[39] See Article 4(4) of the EU-US TFTP Agreement.

The designated provider must then provide the data directly to the U.S. Treasury Department.[40]

The EU-US TFTP Agreement came into force in August 2010. Its implementation is subject to periodic reviews by a Joint Supervisory Body (JSB), composed of representatives of national data protection authorities. The first report of the Joint Supervisory Body was particularly critical about its implementation.[41] More globally, it has been argued that the scrutiny role granted to Europol in the EU-US TFTP Agreement **raises legal basis concerns, as well as effectiveness and human rights issues**.[42]

In 2013, the European Parliament adopted a non-binding resolution calling for the EU to suspend its TFTP agreement with the US in response to the revelations in the press about the access to SWIFT data by the U.S. National Security Agency.[43] The Resolution noted that a majority of the European Parliament had given its consent to the TFTP Agreement solely on account of a strong protection afforded with a view to safeguarding EU citizens' privacy and personal data protection rights, but that, as indicated by the Article 29 Data Protection Working Party, procedures in place for exercising the right of access may not be adequate and in practice it may not be possible to exercise the right to rectification, erasure and blocking.[44]

As it is further argued below, this model is equally problematic from the standpoint of EU legal standards. A key weakness with the role of Europol in the TFTP is the lack of proper oversight and independent scrutiny of decisions. **The obstacles as regards the transparency and accountability of Europol's role** have even been experienced by the European Ombudsman, which has recently been refused public access to a report of Europol's Joint Supervisory Body (JSB) on the implementation of the EU-US TFTP.[45] The challenge of this model remains the lack of independent judicial oversight of decisions taken for access to and transfers of financial data.

---

[40] See Article 4(6) of the EU-US TFTP Agreement.

[41] EUROPOL Joint Supervisory Body, Report on the inspection of EUROPOL's implementation of the TFTP agreement, conducted in November 2010, JSB EUROPOL inspection report 11-07, 1 March 2011, Brussels. On controversies surrounding this agreement, see more generally: Didier Bigo et al. (2011), "Towards a New EU Legal Framework for Data Protection and Privacy: Challenges, Principles and the Role of the European Parliament" (Policy Department C on Citizens' Rights and Constitutional Affairs of the Directorate General for Internal Policies of the European Parliament), especially pp. 74-78.

[42] V. Mitsilegas (2014), "Transatlantic counterterrorism cooperation and European values: The elusive quest for coherence", in E. Fahey and D. Curtin (eds), *A Transatlantic Community of Law*, Cambridge: Cambridge University Press, pp. 289-315.

[43] European Parliament, Resolution of 23 October 2013 on the suspension of the TFTP agreement as a result of US National Security Agency surveillance, P7_TA(2013)0449.

[44] Ibid., paragraphs D and F.

[45] Refer to http://www.ombudsman.europa.eu/en/cases/correspondence.faces/en/59133/html.bookmark.

SECTION 3. APPLICABLE LEGAL INSTRUMENTS AND STANDARDS

KEY FINDINGS

- The EU has exercised wide legal competences and adopted a large set of legal instruments providing common Union standards and benchmarks for assessing the legality of third-country access to data for law enforcement and criminal justice investigations.
- The Treaty of Lisbon reinforced and expanded EU powers as well as democratic and judicial scrutiny in criminal justice and police cooperation domains. The legally binding nature of the EU Charter of Fundamental Rights positions the fundamental rights of individuals at the centre of gravity of the Union's Area of Freedom, Security and Justice.
- EU data protection *acquis* gives a special role to the consent of the data subject as a legitimate ground for accessing and processing data. When moving within the framework of law enforcement and criminal justice activities, MLA agreements laid down the rules for access to be lawful and legitimate, which encompass prior consent by the designated central authority of the requested state and legal scrutiny by an independent judicial authority which will validate the legitimacy and legality of accessing and processing electronic data.

What are the applicable EU legal standards in a post-Lisbon Treaty landscape? This section provides a detailed overview of the main EU legal instruments with direct relevance when assessing the legality of access to data for law enforcement purposes. It starts by providing some conceptual clarifications as regards the relationship between EU data protection and criminal justice *acquis* and fundamental human rights in the EU legal system (section 3.1). It then outlines the standards and benchmarks which they provide in respect of privacy, data protection and the rights of the defence (sections 3.2-3.4). **The EU has extensively exercised legal competence over domains related to privacy, criminal justice and cybercrime, and has developed a large body of law** providing common supranational rule-of-law standards applicable to a large majority of Member States.

3.1. The Circular Relationship between Fundamental Rights, Privacy and Criminal Justice in the EU Legal System

The entry into force of the Lisbon Treaty in December 2009 brought about a **profound reconfiguration of the constitutional foundations of the EU legal system** and the so-called Area of Freedom, Security and Justice (AFSJ).

The Lisbon Treaty meant the expansion of the Community method of cooperation over a majority of European cooperation in criminal justice and police. This injected a higher degree of democratic accountability (European Parliament as co-legislator) and judicial control (Court of Justice of the European Union with jurisdiction to interpret and review EU law) in these domains. It converted the EU Charter of Fundamental Rights into a legally binding instrument, with the same value as the Treaties, and applicable to all European institutions, agencies and EU Member State authorities.

The 'Lisbonisation' of the AFSJ has **reinforced and enhanced EU competence** over areas at the heart of the discussions surrounding access to data for law enforcement and criminal justice purposes. The EU Charter positions **the individual and the protection of fundamental rights and freedoms at the heart of AFSJ cooperation**.[46] Of particular relevance are Articles 7 (Respect of Private and Family Life) and 8 (Protection of Personal Data), as well as those provided under Title VI (Justice), which cover the right to an effective remedy and to a fair trial as well as the rights of the defence.[47]

The Lisbon Treaty led to far-reaching modifications in the architecture of the right to data protection in the EU legal system, both in what concerns primary and secondary law (see section 3.2 below). There is an open debate in the academic literature as regards the reach and scope of the actual difference between the rights to privacy and the one of data protection as enshrined in the EU Charter, and the extent to which the fundamental right of data protection creates a specific and non-derivate system of protection.[48] This discussion falls outside the scope of this study. That notwithstanding, it is important to stress the importance of the right to private life (Article 7 Charter and 8 ECHR) in the development of EU law.

---

[46] S. Carrera and F. Geyer (2008), "The Reform Treaty and Justice and Home Affairs – Implications for the common Area of Freedom, Security and Justice", in E. Guild and F. Geyer (eds), *Security versus Justice? Police and Judicial Cooperation in the European Union*, Aldershot: Ashgate Publishing, pp. 289-307.

[47] S. Peers, T. Hervey, J. Kenner and A. Ward (eds) (2014), *The EU Charter of Fundamental Rights: A Commentary*, Oxford: Hart Publishing.

[48] Ibid., H. Kranenborg Article 8 (Protection of Personal Data), pp. 22-264. For a debate refer to O. Lynskey (2014), "Deconstructing Data Protection: The 'Added Value' of a Right to Data Protection in the EU Legal Order", *International and Comparative Law Quarterly*, Vol. 63, Issue 3, pp. 569-597; See also J. Kokott and C. Sobotta (2013), "The distinction between privacy and data protection in the jurisprudence of the CJEU and the EctHR", *International Data Privacy Law*, Vol. 3, No. 4, pp. 222-228. G. González Fuster and S. Gutwirth (2013), "Opening up Personal Data Protection: A Conceptual Controversy," *Computer Law & Security Review*, 29: 531-39.

What is clear in the current state of EU privacy and data protection *acquis* is **the special role attributed to the consent of the data subject as legitimate key ground for the legitimacy for accessing and processing data**. Article 8 EU Charter stipulates that processing of individuals' data must be on the basis of the consent of the person concerned or some other legitimate grounds foreseen by law. The Data Protection Directive 95/46 also provides that consent constitutes one of the general grounds for lawfulness. The Article 29 Working Party has elaborated some conceptual clarifications as regards the actual reach of 'consent' for the purposes of EU data protection law in its Opinion 15/2011 on the definition of consent.[49]

The legal value of consent in the EU legal system is central at times of examining transnational practices on access to data in European jurisdictions, and the legal dilemmas which they raise. **Who can give consent to access and sharing data?** For the purposes of EU law the answer is the data subject's consent, which goes along the individual rights focus enshrined in the EU Charter.

A broader notion of 'consent' includes the involvement or mediation by **an independent authority in cases where the individual cannot be asked proper consent as the matter is one of criminal justice**, which in most cases will correspond with an authorisation by an independent court of law or judicial authority. The prior consent by the designated central authority in the requested state and the supervision of an independent judicial actor play out a core component of the shapes of MLAs. As we will study in section 3.3 below, they are also at the core of EU criminal justice law, specifically the European Investigation Order (EIO).

The relevance of 'consent', broadly understood, has been confirmed by the Article 29 Working Party's Comments on the issue of unmediated access by third countries' law enforcement authorities to data stored in other jurisdictions, as proposed in the draft elements for an additional protocol to the above-mentioned Budapest Convention on Cybercrime, 5 December 2013, Brussels. When addressing the compliance of the planned revision of the Cybercrime Convention in the Council of Europe, Article 29 WP mentions as one of the key issues of controversy that of "*consent*" and "*whether a private entity could lawfully provide access to or disclose to data*". In its Comments it stated:

> According to the EU data protection *acquis*, **there are two types of consent**: the data subject's consent means 'any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed'…One of the requirements for the consent to be given is that it has to be 'freely given'; this criterion is only fulfilled 'in the absence of negative consequences'. In particular, the Working Party notes that '[c]onsent can only be valid if the data subject is able to exercise a real choice, and there is no risk of deception, intimidation, coercion or significant negative consequences if he/she does not consent'. In a law enforcement

[49] Article 29 Data Protection Working Party, Opinion on the definition of consent 15/2011, 13 July 2011.

> context, however, 'consent' is also understood to be the consent of law enforcement/judicial authorities that need, in relation to a specific case, to exchange data[50] [emphasis added].

In this respect, "*prior consent of the transmitting Member State*" acts as a condition in the Council Framework Decision 2008/977.[51] Furthermore, this has direct implications when examining whether a private entity can lawfully provide access to or disclose the data. The Article 29 WP's Comments emphasise this:

> According to this Directive (95/46), consent can only be given by data subjects. Therefore, companies acting as data controllers usually do not have the 'lawful authority to disclose the data' which they process…They can normally only disclose the data upon prior presentation of a judicial authorisation/warrant or any document justifying the need to access the data and referring to the relevant legal basis for this access, presented by a national law enforcement authority according to their domestic law that will specify the purpose for which data is required. Data controllers cannot lawfully provide access or disclose the data to foreign law enforcement authorities that operate under different legal and procedural framework from both a data protection and a criminal procedural point of view.

This quotation exemplifies one of the key sources of controversy between the EU and the US in respect of access to data. The specificity of the EU data protection and privacy legal system as regards **the conditions for legitimate and lawful grounds for interference to privacy** through access to and processing of data is one where 'consent', broadly understood, in combination with other legitimate grounds and principles (e.g. fairness, necessity and proportionality)[52] play here a crucial role. Moreover, the established transatlantic legal channels of judicial and law enforcement cooperation in the context of criminal investigations place the consent of the requested state (and a designated central authority usually corresponding with the Ministry of Justice), and the scrutiny by an independent and impartial court of law at the heart of the mediated system of access to data.

The point of departure in every evaluation on whether US authorities can have access to or request electronic data directly from private companies in EU law is its incompatibility with the mediated access model provided by the MLA agreement. The role which has been given here to 'consent' by the requested authority and judicial supervision is of profound relevance in safeguarding rule of law and fundamental rights. Direct remote access to electronic data directly challenges these basic foundations, and leaves the door open to arbitrariness, fundamental rights breaches and legal uncertainty.

---

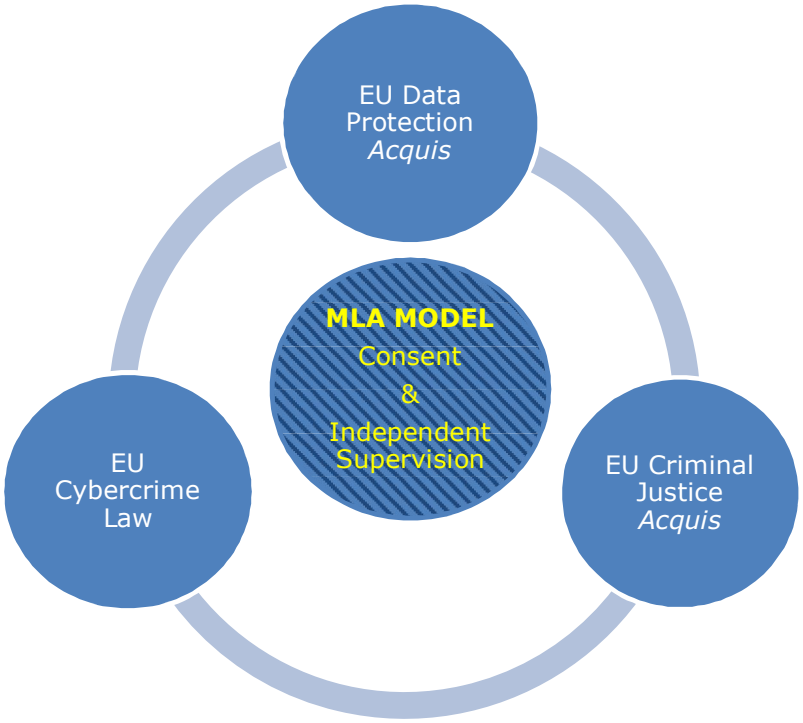
[50] Pp. 2-3.

[51] See footnote 7 of the Article 29 WP Comments.

[52] See p. 7 of the Article 29 Data Protection Working Party, Opinion on the definition of consent 15/2011, 13 July 2011.

All the sources of applicable EU law standards are in this way **intrinsically linked**, in what could be described as a **circular relationship** (see Figure 1 below). That relationship circulates around the question of 'who' can give consent to accessing and sharing data, which is central when testing the legality of third-country access to data held by private companies under EU jurisdiction.[53]

Figure 1. Data Protection, Criminal Justice and Cybercrime: A Circular Relationship



The next sub-sections establish the sector-specific EU legal standards of relevance when testing the legality of third-country access to electronic data held by private companies under EU jurisdiction. They provide a survey (see Table 1 below) of all legal instruments falling within the scope of Union law of relevance when examining the lawfulness of access to and the

[53] In any case, data processed in this context must be regarded as particularly sensitive, taking into account its nature as well as the effects that such data processing or the related data processing may have on individuals. In this sense, see: European Data Protection Supervisor (EDPS), Opinion of the European Data Protection Supervisor on the Initiative of the Kingdom of Belgium, the Republic of Bulgaria, the Republic of Estonia, the Kingdom of Spain, the French Republic, the Italian Republic, the Republic of Hungary, the Republic of Poland, the Portuguese Republic, Romania, the Republic of Finland and the Kingdom of Sweden for a Directive of the European Parliament and of the Council on the European Protection Order, and – on the Initiative of the Kingdom of Belgium, the Republic of Bulgaria, the Republic of Estonia, the Kingdom of Spain, the Republic of Austria, the Republic of Slovenia and the Kingdom of Sweden for a Directive of the European Parliament and of the Council Regarding the European Investigation Order in Criminal Matters (Brussels, 5 October 2010), p. 2.

legitimacy for processing of information for reasons of law enforcement and criminal justice investigations, in particular: EU privacy and data protection law (section 3.2), mutual legal assistance and criminal justice law (section 3.3), and cybercrime law (section 3.4).

Table 1. EU Legal Instruments on Criminal Justice, Privacy and Cybercrime

Criminal Justice	Privacy and Data Protection	Cybercrime
EU Charter of Fundamental Rights (Articles 47-50)	EU Charter of Fundamental Rights (Articles 7 and 8)	Cybercrime Directive (on attacks against information systems)
EU-US Mutual Legal Assistance Agreement	Data Protection Directive	
European Investigation Order (EIO)	E-Privacy Directive	
	Data Retention Directive (annulled)	
	Data Protection Framework Decision	

3.2. Privacy and Data Protection

KEY FINDINGS

- The Council of Europe human rights framework in the European Convention of Human Rights constitutes the starting point when laying down EU privacy and data protection standards for EU Member States.
- The scope of 'private life' under Article 8 ECHR is a broad term, non-susceptible of exhaustive definition. The protection of personal data is 'of fundamental importance' for the enjoyment of this right. Taking privacy as a reference point is most useful when assessing the impact of large-scale access to data on the relationship between the individual and the State.
- One of the most important legal grounds developed by the European Court of Human Rights when examining the legality of States' interferences on privacy and the rights of the defence in a law enforcement context is the 'in accordance with the law test'. This requires a specific quality of the law, which must be sufficiently clear, precise and foreseeable.
- The ECHR-based human right of privacy constitutes a cornerstone in the EU data protection *acquis* and the EU Charter of Fundamental Rights. The fundamental rights of privacy and data protection are granted to *everyone*, not exclusively to EU citizens or residents.

- Article 8.2 EU Charter foresees that data must be processed fairly for specific purposes and on the basis of the unambiguous consent of the person involved or some other legitimate basis laid down by law. 'Consent' plays a central role in the examining the legality and legitimacy of access to data.
- According to the Data Protection Directive 95/46 when data processing activities of private companies fall under EU personal data protection law, these companies cannot freely export personal data to third countries, but must comply with applicable EU norms on cross-border data transfers.
- Lawful access for law enforcement purposes to data held by private companies under EU jurisdiction requires prior review carried out by a court or by an administrative (supervisory) independent body.
- Current and upcoming legal developments on data protection, such as the EU-US umbrella agreement or the EU data protection package, make clear that data held by the private sector shall not be directly accessed by or transferred to US law enforcement authorities outside authorised/formal legal channels of cooperation. The negotiations of the EU-US umbrella agreement are being linked to the need to provide legal protection and effective judicial remedies for EU citizens similar to those for US citizens.

The identification of European standards on privacy and data protection demands recognising **privacy as a primordial human right** in the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) (section 3.1.1). Relevant EU standards on privacy and personal data protection derive from **fundamental rights obligations** enshrined in the EU Charter of Fundamental Rights) and the Treaties, as well as from EU secondary law (section 3.1.2).[54]

3.2.1. Council of Europe

Legal instruments which have been adopted in the Council of Europe are especially relevant for EU law purposes. They also determine **EU Member States' obligations in the area of privacy and personal data protection**. In addition to being crucial to the interpretation of the rights guaranteed by the EU Charter, the ECHR is of the utmost importance for EU law because the EU shall accede to it.[55] Furthermore, all EU Member States are members of the Council of Europe (CoE) and obliged by the ECHR. CoE human rights instruments have been explicitly mentioned in several EU legal acts.[56] They also determine the content of national laws applying to assessing the level of adequate protection of a third country.

[54] See European Union Agency for Fundamental Rights and Council of Europe (2014), Handbook on European Data Protection Law, Publications Office of the European Union, Luxembourg.

[55] Article 6(2) of the Treaty on European Union (TEU).

[56] Article 27 of the Europol Decision.

The most relevant instruments enshrined in the CoE context are: Article 8 ECHR (section 3.1.1.1); the Convention 108 and its Additional Protocol (section 3.1.1.2) and the 1987 Recommendation on the Use of Personal Data in the Police Sector (section 3.1.1.3).

3.2.1.1. Article 8 ECHR

Article 8(1) of the ECHR states that:

> [e]veryone has the right to respect for his private and family life, his home and his correspondence', and its Article 8(2) sets out that '[t]here shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Article 8 ECHR thus explicitly establishes a right to respect for private life, as well as a right to family life, the inviolability of the home and the confidentiality of communications. In recent decades, the European Court of Human Rights (ECtHR) has been detailing the scope of Article 8 ECHR and the necessary requirements for interference to be regarded as lawful and legitimate.

The ECtHR has notably asserted that '**private life' is a broad term not susceptible to exhaustive definition**, and that the protection granted under Article 8 of the ECHR is not limited to the private sphere or the home of the individual.

In *Malone v. the United Kingdom*,[57] the Strasbourg Court examined a case concerning a practice whereby the Post Office provided to the police records about the communications despite the absence of a subpoena to compel the production of such records.[58] The records concerned data obtained through the 'metering' of communications, and thus were not related to the communications' content, but only to the numbers dialled on a particular telephone and the time and duration of each call.[59]

The Court declared that taking into account that the records contained nevertheless "information, in particular the numbers dialled, which is an integral element in the communications made by telephone", the "release of that information to the police without the consent of the subscriber" amounted to an interference with the rights guaranteed by Article 8 of the ECHR.[60] **The disclosure of 'metadata' to law enforcement thus**

---

[57] ECtHR, Malone v. the United Kingdom, App. No. 8691/79, 2 August 1984.

[58] Ibid., para. 86.

[59] Ibid., para. 83.

[60] The Court also noted that there was no rule in domestic law making it unlawful for the Post Office to voluntarily comply with requests from the police to make and supply this type of record, but also no rule delimiting the scope and manner of exercise of the discretion enjoyed by the public authorities, and that as a consequence the interference was not "in accordance with the law". Ibid., paras. 86-87.

constitutes a breach of Article 8 of the ECHR in absence of clear rules delimiting the role of public authorities.

The ECtHR has also specified that e-mails and information derived from the monitoring of Internet usage, including e-mails sent from work and Internet usage at work, are protected under Article 8 of the ECHR in the same way as telephone calls.[61] Telephone, facsimile and e-mail communications are covered jointly by the notions of 'private life' and 'correspondence' within the meaning of Article 8 of the ECHR.[62]

In *Taylor-Sabori v. the United Kingdom*,[63] the applicant's communications had been accessed through a 'clone' of the applicant's pager, and he was subsequently arrested and charged with conspiracy to supply a controlled drug. As at the time there was no provision in British law allowing for such interception, the interference was regarded by the European Court of Human Rights as not being *'in accordance with law'*.

The Strasbourg Court has stressed that the requirement of being ***'in accordance with the law'*** **demands the existence of a provision of domestic law that must have certain qualities**. In *Liberty and others v. the United Kingdom*, observing that the expression 'in accordance with the law' under Article 8(2) requires that the impugned measure should have some basis in domestic law, but also that such basis should be compatible with the rule of law and accessible to the person concerned, "who must, moreover, be able to foresee its consequences for him",[64] the Court assessed that the United Kingdom's legal provisions allowing it to intercept and examine external communications did not meet such requirements.[65] Secret measures of communications surveillance can be in accordance with the requirements of Article 8 of the ECHR if accompanied by some minimum safeguards, to be set out in statute law.[66]

---

[61] ECtHR, Copland v. the United Kingdom, App. No. 62617/00, 3 April 2007, para. 41.

[62] ECtHR, Liberty and others v. the United Kingdom, App. No. 58243/00, 3 April 2007, para. 56.

[63] ECtHR, Taylor-Sabori v. the United Kingdom, App. No. 47114/99, 22 October 2002.

[64] Liberty and others v. the United Kingdom, para. 59. See also Kennedy v. United Kingdom, no. 26839/05, 18 May 2010; Rotaru v. Romania, no. 28341/95, ECHR 2000-V; Amann v. Switzerland, no. 27798/95, ECHR 2000-II; Iordachi and Others v. Moldova, no. 25198/02, 10 February 2009;

[65] More concretely, the Court noted that the domestic law did not indicate "with sufficient clarity, so as to provide adequate protection against abuse of power, the scope or manner of exercise of the very wide discretion conferred on the State to intercept and examine external communications", and, "[i]n particular, it did not, as required by the Court's case-law, set out in a form accessible to the public any indication of the procedure to be followed for selecting for examination, sharing, storing and destroying intercepted material". Ibid., para. 69.

[66] Determining "the nature of the offences which may give rise to an interception order; a definition of the categories of people liable to have their telephones tapped; a limit on the duration of telephone tapping; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which

Therefore, any State interference over human rights provisions in a law enforcement context needs to be firmly anchored in legislation meeting **the following three standards:** first, the practice needs to have its basis in national law; second, the law must be accessible and sufficiently clear and precise to the individual; third, the consequences need to be foreseeable (foreseeability).

The ECtHR has interpreted the scope of Article 8 ECHR as encompassing the compilation of data about individuals by public authorities.[67] **The Court has held in different judgments that the right to private life can be infringed by the collection, registration or use of personal information**.[68] More concretely, the Court has declared that the mere storing of data relating to the private life of an individual amounts to an interference within the meaning of Article 8, and that the subsequent use of the stored information has no bearing on that finding.

In determining whether the personal information retained by the authorities involves any relevant private-life aspects, the Court will have due regard to the specific context in which the information has been recorded and retained, the nature of the records, the way in which these records are used and processed and the results that may be obtained.

The Strasbourg Court has declared that **the protection of personal data** is "*of fundamental importance"* for the enjoyment of the right to respect for private life guaranteed by Article 8 ECHR. Domestic laws must afford appropriate safeguards to prevent any use of personal data that may be inconsistent with its guarantees.[69] The Court has also emphasised that the need for such safeguards "is all the greater where the protection of personal data undergoing automatic processing is concerned, not least when such data are used for police purposes".[70] It has examined multiple situations related to the storage of personal data by public authorities.[71]

In addition, the scope of Article 8 ECHR must be interpreted in accordance with the **Council of Europe's Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108)** (see section 3.2.1.2 below). This implies that storing cards filled with information about individuals obtained

recordings may or must be erased or the tapes destroyed". ECtHR, Weber and Saravia v. Germany (decision as to the admissibility), App. No. 54934/00, 29 June 2006.

[67] See, for instance, ECtHR, Uzun v Germany, App. No. 35623/05, 2 September 2010.

[68] On this subject, see E. Brouwer (2008), Digital Borders and Real Rights: Effective Remedies for Third-Country Nationals in the Schengen Information System, Leiden: Martinus Nijhoff Publishers, pp. 155-176.

[69] See ECtHR, S. and Marper v. the United Kingdom, Nos. 30562/04 and 30566/04, 4 December 2008, § 103.

[70] Ibid.

[71] For example, ECtHR, Leander v. Sweden, No. 9248/81, 26 March 1987.

through the interception of their communications must be regarded as falling under Article 8 ECHR.[72]

The *S. and Marper* case[73] concerned two non-convicted individuals who wanted to have their records removed from a DNA database used for criminal identification in the United Kingdom. Specifically, they asked for their fingerprints, cellular samples and DNA profiles, which had been obtained by police, to be destroyed. In its ruling, the Strasbourg Court established that **it was contrary to the requirements of Article 8 of the ECHR to store for unlimited periods of time that type of personal information related to innocent people in a database of that nature**. The ECtHR concluded that the blanket and indiscriminate nature of the powers granted to UK authorities constituted a disproportionate interference with the applicants' right to respect for private life, and could not be considered necessary in a democratic society, amounting therefore to a violation of Article 8 of the ECHR.

Even when the interception of communications constitutes as such an interference with the rights protected under Article 8 ECHR, the transmission of the obtained data to other authorities has been recognised by the Strasbourg Court as representing a further separate interference with the rights enshrined in Article 8 of the ECHR.[74]

The Strasbourg Court has also specifically acknowledged **the importance of avoiding the use of incorrect personal data in police reporting in criminal proceedings**. In *Cemalettin Canli v. Turkey*,[75] the Court found a violation of Article 8 of the ECHR following the unsuccessful requests made by the applicant to have amended an inaccurate police report submitted to a court in criminal proceedings, as well as police records. The ECtHR explicitly asserted that the information in the police report was within the scope of Article 8 of the ECHR.[76]

3.2.1.2. Convention 108

The Convention for the protection of individuals with regard to the automatic processing of personal data (Convention 108)[77] was historically the first international legally binding instrument dealing with 'data protection', even if only covering the processing of personal data through automated means. Convention 108's scope of application encompasses **all**

---

[72] ECtHR, Amann v. Switzerland, No. 27798/95, 16 February 2000, paras 65-67. ECtHR, Rotaru v. Romania, 28341/95, 4 May 2000. In Rotaru v. Romania, the Court held that any kind of information about individuals, and thus also public information, can fall within the scope of Article 8 of the ECHR when systematically collected and stored in files held by authorities.

[73] ECtHR, S and Marper v. United Kingdom, 30562/04 and 30566/04, 4 December 2008.

[74] Weber and Saravia v. Germany, para. 79.

[75] ECtHR, Cemalettin Canli v. Turkey, No. 22427/04, 18 November 2008.

[76] § 33.

[77] CoE, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Council of Europe, CETS No. 108, 1981.

fields of automated personal data processing and therefore applies to data protection in **the area of police and criminal justice**, even though the contracting parties may limit its application.

Opened for signature in 1981, Convention 108 entered into force in 1985. It has been signed and ratified by all EU Member States, as well as by some other Council of Europe Member States such as Russia, and one non-Member (Uruguay). In 1999 the instrument was amended, allowing the EU to become a Party.[78]

Convention 108 aims "to secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him".[79] Therefore, **it applies generally to *all* individuals whose data is processed**. Convention 108 provides for the free flow of personal data between its parties, but imposes some restrictions on those flows to States where legal regulation does not provide equivalent protection.[80]

In 2001, an Additional Protocol to Convention 108 was adopted and introduced provisions on **transborder data flows to non-parties**, and on the mandatory establishment of national data protection supervisory authorities.[81] It has been ratified by a majority of EU Member States.[82]

The 2001 Additional Protocol to Convention 108 describes transborder data flows as transfers of personal data to a recipient that is subject to the jurisdiction of a State or organisation that is not Party to Convention 108. It establishes that such transfers can only take place **if that State or organisation ensures an *adequate* level of protection for the intended data transfer**.[83]

By way of derogation from such a general rule, each party may nevertheless allow for the data transfer if domestic law allows it because specific interests of the data subject or of "legitimate prevailing interests, especially important public interests", or, still, "if safeguards, which can in particular result from contractual clauses, are provided by the controller responsible for the transfer and are found adequate by the competent authorities according to domestic law".[84]

---

[78] Council of Europe, Amendments to the Convention for the protection of individuals with regard to automatic processing of Personal Data (ETS No. 108) allowing the European Communities to accede, adopted by the Committee of Ministers, in Strasbourg, on 15 June 1999; Article 23 (2) of the Convention 108 in its amended form.

[79] Article 1 of Convention 108.

[80] Article 12 of Convention 108.

[81] Council of Europe, CoE, Additional Protocol to the Convention for the protection of individuals with regard to automatic processing of personal data, regarding supervisory authorities and transborder data flows, CETS No. 181, 2001.

[82] The EU Member States that have not ratified the 2001 Additional Protocol are Belgium, Greece, Italy, Malta, Slovenia and the United Kingdom.

[83] Article 2 (1) of the 2001 Additional Protocol.

[84] Article 2 (2) of the 2001 Additional Protocol.

3.2.1.3. Recommendation No. R (87) 15

In 1987, the Council of Europe's Committee of Ministers adopted a Recommendation on the Use of Personal Data in the Police Sector.[85] It provides guidance for the collection, storage, use and communication of personal data for police purposes that are the subject of automatic processing.

The Recommendation's guidance on "international communication" of data indicates that **the transfer of data to foreign authorities should be restricted to police bodies**, and that it should only be permissible "if there exists a clear legal provision under national or international law", or, in the absence of such a provision, "if the communication is necessary for the prevention of a serious and imminent danger or is necessary for the suppression of a serious criminal offence under ordinary law", but in any case exclusively "provided that domestic regulations for the protection of the person are not prejudiced".[86]

The Council of Europe's Project Group on Data Protection (CJ-PD) has pointed out that **bilateral or multilateral agreements on the exchange of police data** may, **for the purpose of data protection**, contain provisions on the types of data to be transferred, the authorities which could control the data, the prohibition in principle on the transfer of the data to other authorities or private parties, the obligation to ensure the right of data subjects to have information about them and to obtain the correction of their data, the obligation to delete the data after the fulfilment of the purpose for which the data were transferred and to inform each other about the time limit of storage of the data under their law, as well as the possibility for the data subject to have an effective remedy before an independent authority.[87]

3.2.2. EU Fundamental Rights Requirements

Fundamental rights form an integral part of the general principles of EU law, and are currently set out in the Charter of Fundamental Rights of the EU[88] (hereafter, the 'EU Charter').[89] The EU Charter generally reaffirms the rights

---

[85] Recommendation No. R (87) 15 of the Committee of Ministers to Member States regulating the use of personal data in the police sector, adopted by the Committee of Ministers on 17 September 1987.

[86] See Article 5(4) of Recommendation No. R (87) 15.

[87] Project Group on Data Protection (CJ-PD), Report on the Third Evaluation of Recommendation no. R(87) 15 regulating the use of personal data in the police sector, 2002, p. 12.

[88] Charter of Fundamental Rights of the European Union, 30 March 2010, OJ C83, p. 389.

[89] On the key relevance of the EU Charter as a starting point for issues related to EU personal data protection, see CJEU, Case C-131/12, Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González, para. 68. More generally, on the EU Charter refer to G. De Búrca (2013), "After the EU Charter of Fundamental Rights: The Court of Justice as a Human Rights Adjudicator?", *Maastricht Journal of European and Comparative Law*, 20, no. 2, pp. 168-84.

guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) as interpreted in the case law of the European Court of Human Rights, to be taken into account for its interpretation.[90] **EU fundamental rights are generally granted to 'everyone', and not exclusively to EU citizens or EU residents.**

The EU Charter is legally binding since the entry into force of the Lisbon Treaty in December 2009. As established by Article 51(1), its provisions:

> …are addressed to the institutions, bodies, offices and agencies of the Union with due regard for the principle of subsidiarity and to the Member States only when they are implementing Union law. They shall therefore respect the rights, observe the principles and promote the application thereof in accordance with their respective powers and respecting the limits of the powers of the Union as conferred on it in the Treaties.

It is thus **binding on EU institutions, and on Member States when acting within the scope of EU law**. The European Commission oversees respect of the EU Charter by EU Member States, under the control of the CJEU, and can open infringement proceedings in case of breach. All EU law provisions and national law based on EU law must be interpreted by national courts and judges in coherence with EU Charter obligations.

Two main articles of the EU Charter delimit the EU's obligations in relation to privacy and personal data protection: Article 7 and Article 8. Article 7 EU Charter enshrines the rights to respect for private life and the confidentiality of communications; whereas Article 8 lays down a right to the protection of personal data.[91]

3.2.2.1. Article 7 EU Charter

Article 7 establishes that "[e]veryone has the right to respect for his or her private and family life, home and communications". This provision corresponds to Article 8 of the ECHR, and shall thus be interpreted accordingly and take into account the case law of the ECtHR,[92] which has notably asserted that 'private life' is a broad term not susceptible to exhaustive definition (see section 3.1.1.1 above).

The European Court of Human Rights case law on Article 8 of the ECHR provides crucial guidance on its scope and the requirements applicable to lawful interferences with the right to respect for private life. The Court of Justice of the European Union (CJEU) in Luxembourg has notably asserted

---

[90] Article 6(1) of the Treaty on European Union (TEU).

[91] The rights protected under Articles 7 and 8 of the EU Charter can be limited in accordance with the requirements detailed in Article 52(1) of the EU Charter, which states: "Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others".

[92] The first sentence of Article 52(3) states: "In so far as this Charter contains rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, the meaning and scope of those rights shall be the same as those laid down by the said Convention".

the relevance of Article 8 of the ECHR and the right to privacy for the interpretation of EU personal data protection in 2003, in the *Rundfunk* judgment.[93]

3.2.2.2. Article 8 EU Charter

Article 8(1) of the EU Charter sets out that:

> [e]veryone has the right to the protection of personal data concerning him or her'. Article 8(2) adds that '[s]uch data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law', and that '[e]veryone has the right of access to data which has been collected concerning him or her, and the right to have it rectified'. Finally, Article 8(3) establishes that '[c]ompliance with these rules shall be subject to control by an independent authority'.

The fundamental right to the protection of personal data is also enshrined in the EU Treaties.[94] The EU fundamental right to the protection of personal data foresees that personal data can only be processed for specified purposes.[95]

The right to the protection of personal data also sets out that personal data can only be processed **on the basis of legitimate grounds laid down by law, or the consent of the individual concerned**. This relates to the principle that lawful processing can only take place on the basis of a legitimate ground. Such ground might be the consent of the individual, but otherwise it must be a ground laid down by a law.

The need for a legitimate ground in order to process personal data applies generally to any data processing activity, which can include the collection, storage, and making available or accessing data. Therefore, it is not only necessary, for instance, for a private company to base its processing and eventual storage of data on a legitimate ground (consent or a ground laid down by law); if a public authority wishes to access the data held by the private company, such access shall also be based on a legitimate ground (consent or a ground laid down by law).

The right to the protection of personal data also establishes that when personal data are processed the individuals concerned have a **right to access, and a right to correct, inaccurate data**, and that compliance with personal data protection rules needs to be monitored by **an**

---

[93] CJEU, Rechnungshof (C-465/00) v. Österreichischer Rundfunk and Others and Christa Neukomm (C-138/01) and Joseph Lauermann (C-139/01) v. Österreichischer Rundfunk, Judgment of the Court of 20 May 2003, notably paragraph 68.

[94] See Article 16(1) of the Treaty on the Functioning of the European Union (TFEU). On this right, see also G. González Fuster (2014), *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, Dordrecht: Springer.

[95] Purpose specification is one of the basic principles of European data protection law. It consolidates a link between the legitimacy of personal data processing to the limitation of the aims of the processing: any personal data processing without a clearly defined purpose shall be regarded as unlawful.

independent data protection authority.[96] The case law of the ECtHR on the limitations related to data processing developed under Article 8 of the ECHR is directly relevant for the interpretation of Article 8 of the EU Charter.[97]

3.2.2.3. EU Secondary Law on Data Protection

EU secondary law on personal data protection is profoundly marked by the legacy of the EU's evolution. The main EU data protection instrument does not apply to data processing in the area of police and judicial cooperation in criminal matters, which is only regulated at EU level in the context of cross-border data processing.

a. Data Protection Directive

A key legal instrument in EU secondary legislation is Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive).[98] The Data Protection Directive aimed at harmonising data protection in the single market. The Court of Justice of the European Union has asserted that harmonisation of national laws is "generally complete",[99] which limits the possibilities for EU Member States to depart from its provisions.

The Data Protection Directive's Preamble proclaims that data processing systems must, "whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably the right to privacy".[100] In accordance with the Directive, **Member States shall thus protect the fundamental rights and freedoms of *all* natural persons**, and in particular their right to privacy with respect to the processing of personal data.[101]

---

[96] The EU Court of Justice has underlined the importance of the independence requirement, and has ruled several times on the issue. See: CJEU, C-518/07, European Commission v. Federal Republic of Germany, 9 March 2010; CJEU, C-288/12, European Commission v. Hungary, 8 June 2012; CJEU, C-614/10, European Commission v. Republic of Austria, 16 October 2012.

[97] Noting that it is not extraordinary for the CJEU to refer to the case law of the European Court of Human Rights in cases where the rights to respect for private life and personal data protection under Articles 7 and 8 of the EU Charter apply: Legal Service of the European Parliament (2015), Legal Opinion in Reference to Questions Relating to the Judgment of the Court of Justice of 8 April 2014 in Joined Cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and Others – Directive 2006/24/EC on Data Retention – Consequences of the Judgment, p. 9.

[98] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L281, 23.11.1995, pp. 31-50.

[99] CJEU, Joined cases C-468/10 and C-469/10, Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) and Federación de Comercio Electrónico y Marketing Directo (FECEMD) v. Administración del Estado, 24 November 2011, paras 28-29.

[100] Recital (2) of Directive 95/46/EC.

[101] Article 1(1) of Directive 95/46/EC.

The material scope of the Data Protection Directive does not include matters of police and criminal justice cooperation.[102] Directive 95/46/EC was adopted in 1995 as an internal market instrument, exclusively dealing with processing activities falling under Community law.

For the purposes of the Data Protection Directive, the location of data is not as such a criterion to determine territorial applicability. National provisions implementing the Data Protection Directive apply to any processing carried out in the context of **the activities of an establishment of a data controller on the territory of an EU Member State**.[103] They also apply if the data controller is not established on the Member State's territory, but in a place where the Member State's national law applies by virtue of international public law.[104] And if the data controller is not established on EU territory but, nevertheless, makes use, for the purpose of processing personal data, of equipment situated on the territory of a Member State, the Data Protection Directive shall also apply, unless such equipment is used only for purposes of transit through EU territory.[105]

The Court of Justice of the European Union (CJEU) has stressed that EU personal data protection law must be interpreted as to offer effective and complete protection of data subjects, that is, of the individuals whose personal data is processed. In May 2014, the Luxembourg Court emphasised that Directive 95/46/EC prescribes a "particularly broad territorial scope" in order to prevent individuals from being deprived of protection.[106] The CJEU declared that, in light of the Directive's objective of ensuring effective and complete protection of the fundamental rights and freedoms of natural persons, its provisions on territorial scope of application "cannot be interpreted restrictively".[107]

The territorial application of EU data protection law cannot be interpreted narrowly, as it pursues the delivery of effective and complete protection of data subjects. When data processing activities of private companies fall under EU personal data protection law, **these companies cannot export personal data to third countries, but must comply with applicable EU norms on cross-border data transfers**. Here, the basic rule is that data transfers to any countries outside the EU[108] shall be in principle forbidden, unless the third country provides for an "adequate level" of

---

[102] Article 3(2) of Directive 95/46/EC.

[103] Article 4(1)(a) of Directive 95/46/EC.

[104] Article 4(1)(b) of Directive 95/46/EC.

[105] Article 4(1)(c) of Directive 95/46/EC.

[106] Case C-131/12, Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, Judgment of the Court (Grand Chamber) of 13 May 2014, § 53.

[107] Google Spain SL and Google Inc., para. 54.

[108] The reference to the EU must be understood here as encompassing all European Economic Area (EEA) countries, that is, including Iceland, Liechtenstein and Norway, as the territorial application of the Data Protection Directive reaches beyond the 28 EU Member States.

protection.[109] Article 25(1) of the Data Protection Directive sets out indeed that, in principle, "the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer" may take place only if the third country in question ensures an adequate level of protection.[110]

It is possible to transfer data to third countries that have not been recognised as providing an adequate level of protection if the data controller adduces additional safeguards (for instance, by using contractual clauses or Binding Corporate Rules, BCRs), [111] adopts standard contractual clauses,[112] or refers to one of the six derogations listed in Article 26(1) of Directive 95/46/EC, such as **the data subject's unambiguous consent**,[113] or the fact that the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims.[114]

The US is not regarded as providing an adequate level of protection for personal data in light of EU standards. To facilitate data transfers to the US despite this fact, the U.S. Department of Commerce in consultation with the European Commission developed in 2000 a 'Safe Harbour' framework, which the European Commission considered as providing an adequate level of protection. The Safe Harbour framework is based on self-certification, and allows companies committing to a series of principles to be able to transfer personal data from the EU to the US.

The protection granted by the Safe Harbour approach, nevertheless, has since then been questioned. In 2013, the European Commission recommended that privacy policies of self-certified companies "should include information on the extent to which US law allows public authorities to collect and process data transferred under the Safe Harbour", [115] and that companies "should be encouraged to indicate in their privacy policies when they apply exceptions…to meet national security, public interest or law enforcement requirements".[116]

A case is currently pending before the CJEU, on whether the European Commission's decision creating the EU-US Safe Harbour is (still) valid in

---

[109] Article 25(1) of Directive 95/46/EC.

[110] Article 25(1) of the Directive 95/46/EC.

[111] Article 26(2) of Directive 95/46/EC.

[112] Article 26(4) of Directive 95/46/EC.

[113] Article 26(1)(a) of Directive 95/46/EC.

[114] Article 26(1)(d) of Directive 95/46/EC.

[115] European Commission, Communication to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU, COM(2013) 847 final, Brussels, 27.11.2013, p. 19.

[116] Ibid.

light of revelations regarding mass surveillance by US authorities.[117] In the meantime, a new Safe Harbour agreement is being discussed between the US and the EU.

b. E-Privacy Directive

Directive 2002/58/EC on the processing of personal data and the protection of privacy in the electronic communications sector (e-Privacy Directive)[118] was adopted in 2002 to complement and particularise the provisions of the Data Protection Directive for the telecommunications sector.

The e-Privacy Directive imposes on Member States the obligation to ensure through national legislation **the confidentiality of communications and related 'traffic data' by means of public communications networks and publicly available electronic communications services**.[119] 'Traffic data' are defined as any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof.[120]

Listening, tapping, storing or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, is only possible when legally authorised in accordance with Article 15(1) of the e-Privacy Directive. By virtue of Article 15(1), Member States may adopt laws restricting the scope of rights of individuals:

> …when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system.[121]

---

[117] Case C-362/14, Maximillian Schrems v. Data Protection Commissioner, reference for a preliminary ruling from the High Court of Ireland (Ireland) made on 25 July 2014.

[118] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, OJ [2002] L201, as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No. 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, OJ [2009] L337.

[119] Article 15 of Directive 2002/58/EC.

[120] Article 2(b) of Directive 2002/58/EC. The e-Privacy Directive also uses the notion of 'location data', referring to traffic data related to the location of the communication device.

[121] The provision also refers to Article 13(1) of Directive 95/46/EC, which authorises the Member States to adopt legislative measures to restrict the obligation of confidentiality of personal data where that restriction is necessary, *inter alia*, for the protection of the rights and freedoms of others.

The provision specifies that to such end Member States may adopt laws providing for the retention of data for a limited period of time. Any national measures, however, *"shall be in accordance with the general principles of Community law"*, including fundamental rights.

c. The invalidated Data Retention Directive

In 2006, Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks (the 'Data Retention Directive')[122] transformed the possibility granted by Article 15(1) of the e-Privacy Directive into an obligation. More concretely, it obliged communication service providers to keep traffic data for a period of at least six but not more than 24 months, and to make available such data to law enforcement authorities for the purposes of fighting serious crime.

On 8 April 2014, the CJEU ruled in **the Digital Rights Ireland ruling** that the Data Retention Directive was invalid for infringements of the fundamental rights to privacy and protection of personal data guaranteed by Articles 7 and 8 of the Charter.[123] More concretely, it held that the interference by the Data Protection Directive with the fundamental rights to respect for private life and to the protection of personal data was not limited to what is strictly necessary.

The Court confirmed that the amount and precision of the data covered by the Data Retention Directive allowed very precise conclusions to be drawn concerning people's private lives. **This conflicted with the right to respect for private life (as protected by Article 7 of the EU Charter) and it therefore must be considered to be particularly serious interference**. The CJEU held that access to and collection of metadata is not an interference with privacy simply because the authorities do not have access to the content of communications such as e-mails and phone conversations.[124]

In this sense, the Luxembourg Court noted that Directive 2006/24/EC did not lay down any objective criterion by which the number of persons authorised to access and subsequently use the data retained was limited to what is strictly necessary in the light of the objective pursued. *"Above all"*, states the judgment, the access by competent national authorities to the data was problematically

---

[122] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (Data Retention Directive), OJ [2006] L105.

[123] CJEU, Joined Cases C-293/12 and C-594/12, Digital Rights Ireland Ltd and Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl and others. The judgment was delivered in response to two requests for preliminary rulings.

[124] For the EU now, access to or collection of 'metadata' is by definition an invasion with privacy. See E. Guild and S. Carrera (2014), "The Political and Judicial Life of Metadata: Digital Rights Ireland and the Trail of the Data Retention Directive", CEPS Liberty and Security Series, Centre for European Policy Studies, Brussels.

> not made dependent on a prior review carried out **by a court or by an independent administrative body** whose decision seeks to limit access to the data and their use to what is strictly necessary for the purpose of attaining the objective pursued and which intervenes following a reasoned request of those authorities submitted within the framework of procedures of prevention, detection or criminal prosecutions[125] (emphasis added).

Access for law enforcement purposes to data held by private companies thus imperatively requires the prior review of carried out by a court or by an administrative independent body.

d. Data Protection Framework Decision

The Council's Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (the 'Data Protection Framework Decision')[126] aims at providing protection of personal data when processed for the purpose of preventing, investigating, detecting or prosecuting a criminal offence or of executing a criminal penalty. The scope of application of the Framework Decision is limited to cross-border cooperation between authorities, and thus applies only to data obtained in the course of cross-border cooperation. It does not encompass national security.

The Framework Decision foresees that **the receiving Member State must respect any restrictions on further exchange of data established in the law of the transmitting Member State**. Onward transfer of data to competent authorities in third countries requires the consent of the Member State from which the data originate, although there are exemptions foreseen for urgent cases. Such onward transfer can in principle only take place **if the third country concerned ensures an adequate level of protection for the intended data processing**,[127] a level of adequacy to be assessed taking into account the nature of the data, the purpose and duration of the processing, the country of origin and the country of final destination of the data, the rules of law in force in the third country in question and the professional rules and security measures which apply.[128]

By way of derogation from the general requirement of providing an adequate level of protection, personal data might be transferred to a third country regarded as generally not providing an adequate level if the national law of the transferring Member State allows it because of **a legitimate specific interest** of the data subject or "legitimate prevailing interests, especially important public interests", or still if the receiving third

---

[125] Digital Rights Ireland, para. 62. The prior review body should consider every request for access to the data following a reasoned request from the law enforcement authorities seeking access in order to ensure that the access, if permitted, is strictly necessary to achieve only the identified legitimate objective.

[126] Council of the European Union (2008), Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, OJ 2008 L350.

[127] Article 13(1)(d) of Framework Decision 2008/977/JHA.

[128] Article 13(4) of Framework Decision 2008/977/JHA.

country "provides safeguards which are deemed adequate by the Member State concerned according to its national law".[129]

Framework Decision 2008/977/JHA has been an extremely controversial legal instrument since its adoption, due its limited scope of application, the weak level of protection it establishes,[130] and its regulation of transfers of personal data to third countries. The instrument's limitations appear particularly problematic in a post-Lisbon perspective,[131] notably taking into account the collapse of the EU's 'Third Pillar' and the existence of a legal basis in EU treaties alluding to need to regulate data protection across EU law.

3.2.2.4. Current and Upcoming developments

There are a series of important forthcoming instruments currently being discussed, with important implications for EU privacy and personal data protection for the purposes of this study. These developments mirror the need to ensure efficient safeguards for the fundamental rights to the protection of privacy and personal data in light of the ongoing proliferation of personal data processing and the 2013 revelations on worldwide surveillance programmes.[132]

a. The 'umbrella' agreement

The EU and the US have been negotiating an agreement on the protection of personal data when transferred and processed for the purpose of preventing, investigating, detecting or prosecuting criminal offences, including terrorism, in the framework of police and judicial cooperation in criminal matters. This instrument is commonly referred to as the EU-US 'umbrella' agreement.

Negotiations on this agreement have been ongoing since 2010, when they were launched based on work previously undertaken by the High-Level Contact Group on Information-Sharing and Privacy and Personal Data Protection (HLCG). The HLCG, established in 2006, had presented a final report in 2008, followed by an addendum in 2009. Documents from the Council on the umbrella agreement are only partially declassified.[133] The

---

[129] Article 13(3) of Framework Decision 2008/977/JHA.

[130] On this subject, see H. Hijmans and A. Scirocco (2009), "Shortcomings in EU Data Protection in the Third and the Second Pillars: Can the Lisbon Treaty Be Expected to Help?," *Common Market Law Review*, 46, pp. 1485- 1525 (especially p. 1494).

[131] In this sense, see for instance M. O'Neill (2010), "The Issue of Data Protection and Data Security in the (Pre-Lisbon) EU Third Pillar", *Journal of Contemporary European Research*, Vol. 6, No. 2, pp. 211-235.

[132] European Commission, Report from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: 2014 Report on the Application of the EU Charter of Fundamental Rights, COM(2015) 191 Final (Brussels, August 5, 2015), pp. 12-13.

[133] Council of the EU, Partial declassification of document 12408/10 RESTREINT UE dated 23 July 2010, Brussels, 22 September 2010, 12408/10 EXT 1 JAI 645 DAPIX 10 US 100 DATAPROTECT 59 RELEX 667.

negotiations are believed to be currently waiting for progress on what has been identified as the main outstanding issue for the EU, which is **to provide EU citizens who are not resident in the US the right to judicial redress if their data has been mishandled**.[134]

The commitment of the European Commission to conclude the negotiations of the 'umbrella' agreement, and the importance of securing procedural safeguards for EU citizens, were further emphasised in the Communication adopted by the Commission in 2013 as a reaction to the Snowden revelations, *Rebuilding trust in EU-US data flows.*[135] The Communication noted that the notion of 'EU citizens' must be understood as encompassing also non-EU citizens falling under the scope of EU personal data protection law.[136]

According to the *Rebuilding trust in EU-US data flows* Communication, the negotiations of the 'umbrella' agreement provide an opportunity for the EU to make clear that personal data held by private companies and located in the EU shall not be directly accessed by or transferred to US law enforcement authorities outside of formal channels of cooperation such as MLA or sector-specific agreements – unless in "clearly defined, exceptional and judicially reviewable situations".[137] The European Commission added that the US should undertake clear commitments in this regard.[138]

b. Review of EU Data Protection Framework

The EU personal data protection legal landscape is being reviewed. The European Commission introduced in 2012 a legislative package consisting of two proposals accompanied by a Communication.[139] The first is a proposal for a Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (proposal for a General Data Protection Regulation),[140] introduced to replace Directive 95/46/EC.

---

[134] Joint Press Statement following the EU-US-Justice and Home Affairs Ministerial Meeting of 18 November 2013 in Washington, D.C., European Commission, 18 November 2013.

[135] European Commission, Communication to the European Parliament and to the Council: Rebuilding Trust in EU-US Data Flows, COM(2013) 846 final, Brussels, 27.11.2013, p. 10.

[136] Ibid., p. 2.

[137] Ibid., p. 8.

[138] Ibid.

[139] European Commission, Safeguarding Privacy in a Connected World: A European Data Protection Framework for the 21st Century, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, COM(2012) 9 final, Brussels, 25.1.2012.

[140] European Commission, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11 final, Brussels, 25.1.2012.

The second is a proposal for a Directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data,[141] put forward to replace Framework Decision 2008/977/JHA. The legislative package is based on Article 16 of the Treaty on the Functioning of European Union (TFEU).[142]

In March 2014, the European Parliament adopted a compromise text of the proposed EU General Data Protection Regulation[143] and on the proposed Directive,[144] endorsing versions previously approved by its Committee on Civil Liberties, Justice and Home Affairs in 2013.

After the Council adopted a general approach on the proposed General Data Protection Regulation, trilogue negotiations between representatives of the Council and the European Parliament, together with the European Commission, were launched in June 2015 and should be concluded by the end of 2015. The Council aims at reaching a general approach on the proposed Directive in autumn 2015, allowing the start trilogue meetings on the Directive that would then run in parallel with those on the Regulation.

c. Proposed General Data Protection Regulation

In the 2013 report on the proposed General Data Protection Regulation of the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE), the rapporteur, Jan Philipp Albrecht, declared he strongly regretted that the European Commission's proposed draft Regulation failed to cover law enforcement cooperation, leaving "legal uncertainty as regards rights and obligation in borderline issues, for instance where commercial

---

[141] European Commission, Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, COM(2012) 10 final, 25.1.2012, Brussels.

[142] Article 16 TFEU states, "Everyone has the right to the protection of personal data concerning them" and that "[t]he European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data".

[143] European Parliament legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)).

[144] European Parliament legislative resolution of 12 March 2014 on the proposal for a directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data (COM(2012)0010 – C7-0024/2012 – 2012/0010(COD)).

data is accessed by law enforcement authorities for law enforcement purposes and transfers between authorities that are responsible for law enforcement and those that are not".[145]

The draft General Data Protection Regulation proposed by the European Commission revises the criteria applicable to determining **the territorial scope of application of EU personal data protection law**. The criterion of the establishment of the controller is maintained. The criterion of the use of equipment is abandoned, and introduced instead is a provision stating that the Regulation shall apply "to the processing of personal data of data subjects residing in the Union by a controller not established in the Union, where the processing activities are related to: (a) the offering of goods or services to such data subjects in the Union; or (b) the monitoring of their behaviour".[146]

This could be perceived as an attempt to widen the territorial scope of EU personal data protection law, as **the Regulation shall be applicable when a company targets European consumers even if it does not use equipment based in the EU**. The limitation of protection to the data of individuals residing in the EU introduces, however, an unprecedented limitation of the scope of an EU personal data protection instrument.

Regarding the regulation of data transfers to third countries, the Preamble to the proposed General Data Protection Regulation, in the draft introduced by the European Commission, declares: "Some third countries enact laws, regulations and other legislative instruments which purport to directly regulate data processing activities of natural and legal persons under the jurisdiction of the Member States", [147] adding, "[t]he extraterritorial application of these laws, regulations and other legislative instruments may be in breach of international law and may impede the attainment of the protection of individuals guaranteed in the Union by this Regulation".[148]

In this context, it indicates that only transfers meeting the applicable conditions set out by the Regulation shall be allowed, which may be the case "where the disclosure is necessary for an important ground of public interest recognised in Union law or in a Member State law to which the controller is subject".[149]

Discussions at the Council of the EU have showed that some EU Member States delegations question the relevance of the 'adequate protection' approach, taking into account that in practice manifold exceptions included

---

[145] See Explanatory Statement of Report of 22 November 2013 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)), Committee on Civil Liberties, Justice and Home Affairs, Rapporteur: Jan Philipp Albrecht.

[146] Article 3(2) of the proposed General Data Protection Regulation.

[147] COM(2012) 11 final, p. 31.

[148] Ibid.

[149] Ibid.

in the proposed Regulation would empty the rule of its meaning.[150] Furthermore, some national delegations have questioned the feasibility of maintaining an adequacy test in reference to massive flows of personal data in the context of cloud computing, asking whether a transfer of data in that context or the disclosure of data on the Internet shall be regarded as a transfer of data.[151]

In March 2014, the European Parliament adopted a legislative resolution on the proposed General Data Protection Regulation, putting on the table a proposed new Article, Article 43a, on "Transfers or disclosures not authorised by Union law". The first paragraph of the proposed Article states:

> No judgment of a court or tribunal and no decision of an administrative authority of a third country requiring a controller or processor to disclose personal data shall be recognized or be enforceable in any manner, *without prejudice to a mutual legal assistance treaty or an international agreement in force between the requesting third country and the Union or a Member State* (emphasis added).
>
> [While the second adds that] Where a judgment of a court or tribunal or a decision of an administrative authority of a third country requests a controller or processor to disclose personal data, the controller or processor and, if any, the controller's representative, shall notify the supervisory authority of the request without undue delay and must obtain prior authorisation for the transfer or disclosure by the supervisory authority.

The two remaining paragraphs of the proposed Article 43a detail the procedure to be followed by the supervisory authority, which includes **the possibility to foresee informing the affected data subjects**.[152] The position adopted by the European Parliament thus accepts the possibility that a court or tribunal or a decision of an administrative authority of a third country requests a controller or processor to disclose personal data outside mutual legal assistance treaties or other international agreements, but **conditions acceptance of such requests to a prior authorisation by a supervisory authority**.

---

[150] Council of the EU, Note on Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), 9398/15, Brussels, 1 June 2015, p. 181.

[151] Ibid.

[152] "The supervisory authority shall assess the compliance of the requested disclosure with the Regulation and in particular whether the disclosure is necessary and legally required in accordance with points (d) and (e) of Article 44(1) and Article 44(5). Where data subjects from other Member States are affected, the supervisory authority shall apply the consistency mechanism referred to in Article 57", and "The supervisory authority shall inform the competent national authority of the request. Without prejudice to Article 21, the controller or processor shall also inform the data subjects of the request and of the authorisation by the supervisory authority and where applicable inform the data subject whether personal data was provided to public authorities during the last consecutive 12-month period, pursuant to point (ha) of Article 14(1)".

d. Proposed Data Protection Directive

The European Parliament adopted also in March 2014 a legislative resolution proposing to amend the draft Data Protection Directive to clarify the requirements applicable to the use for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties of data initially processed for other purposes.

The proposed Article 43a states that competent authorities may only have access to personal data initially processed for other purposes only if "specifically authorised by Union or Member State law" meeting necessity requirements and that shall provide that access is limited to authorised staff of the competent authorities in the performance of their tasks "where, in a specific case, reasonable grounds give reason to believe that the processing of the personal data will substantially contribute to the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties", that requests for access be in writing and refer to the legal ground for the request, that the written request be documented; and that "appropriate safeguards are implemented to ensure the protection of fundamental rights and freedoms in relation to the processing of personal data…without prejudice to and complementary to specific conditions of access to personal data such as judicial authorisation in accordance with Member State law". The proposed provision further states, "Personal data held by private parties or other public authorities shall only be accessed to investigate or prosecute criminal offences in accordance with necessity and proportionality requirements", as defined by EU and national laws.

3.3. Mutual Legal Assistance and Criminal Justice Law

KEY FINDINGS

- Article 47 EU Charter stipulates a right to an effective remedy and fair trial before a tribunal. It therefore underlines the judicial nature of the scrutiny when examining the legality of States' interferences with the rights of defence in criminal procedures.
- Supranational cooperation and assistance in criminal law matters have been settled in Mutual Legal Assistance Treaties (MLAT). A case in point is the 2003 EU-US MLA.
- The EU-US MLA constitutes a flexible tool for cooperation, which sometimes provides an excessively broad basis for exchange of information and a number of exceptions allowing for a wide array of judicial assistance options. The Agreement contains a rather weak data protection framework, thus privacy concerns rarely constitute a barrier to cooperation.
- The emphasis given by the EU-US MLA to the maintenance or establishment of bilateral relations between EU Member States and the US does not negate EU Member States' obligations under EU law. The EU-US agreement is a full supranational EU agreement. It must be therefore interpreted in light of EU primary (Treaty) law, the EU Charter of Fundamental Rights as well as European secondary legislation.

- The European Investigation Order (EIO) regulates the exchange of evidence between EU Member States in the area of criminal justice. It introduces a system of 'mutual recognition' based on a minimum of formalities and speed.
- The EIO represents a benchmark for future internal and external EU action in the area of access to data and evidence in judicial cooperation in criminal matters. While the EIO model allows for the procedures for exchanging evidence between EU Member States, it also provides the necessary safeguards for guaranteeing the rule of law and fundamental rights protection. It does so by including a set of provisions preventing automatic mutual recognition and making cooperation subject to States' legal and constitutional systems, proportionality and fundamental rights tests, and the involvement of independent judicial authorities.

A second set of EU legal standards relates to criminal justice in the form of international agreements and secondary legislation. Title VI of the EU Charter of Fundamental Rights (Justice)[153] provides the basis upon which these instruments need to be interpreted and applied in practice. Of particular relevance for the scope of this study is Article 47 EU Charter. This provision stipulates a right to an **effective remedy and fair trial**:

> Everyone whose rights and freedoms guaranteed by the law of the Union are violated has the right to an effective remedy before a tribunal. Everyone is entitled to a fair trial and public hearing within a reasonable time by an independent and impartial tribunal previously established by law…

The *judicial* nature of scrutiny finds its foundations in CJEU case law, which has previously considered judicial accountability a general principle of EU law.[154] In the light of this, the relevance of effective and open justice, as well as effective judicial scrutiny, constitutes a central component of the EU legal system when assessing the legality and legitimacy of law enforcement and criminal justice authorities' interferences with EU Charter rights. This is even the case in situations where the notion of 'national security' is alleged as the justification for that interference by State authorities.[155]

Supranational cooperation in criminal justice investigations and proceedings has been developed between the EU and third countries in international treaties which have taken the shape of **Mutual Legal Assistance (MLA) agreements**. This has been the case most notably for the purposes of this study in relation to the EU-US Agreement on Mutual Legal Assistance, which has been already introduced above (section 3.2.1).[156]

---

[153] P. Aalto et al. (2014), "Article 47 – Right to an Effective Remedy and to a Fair Trial", in S. Peers, T. Hervey, J. Kenner and A. Ward (eds), *The EU Charter of Fundamental Rights: A Commentary*, Oxford: Hart Publishing, p. 1208.

[154] Case 222/84 Johnston [1986] ECR 1651.

[155] D. Bigo et al. (2014), "National Security and Secret Evidence in Legislation and Before the Courts: Exploring the Challenges", CEPS Liberty and Security in Europe Series, Centre for European Policy Studies, Brussels.

[156] See section 2.1 of this Study on mediated access model.

Furthermore, the EU has striven to develop during the last 15 years a **European Criminal Justice Area**.[157] This political goal has been based on the presumption of mutual trust between EU Member States and their authorities, as well as the principle of mutual recognition of criminal justice decisions. One of the latest steps forward in the domain of judicial cooperation in criminal matters at EU level has been the adoption of the European Investigation Order in 2014 (section 3.2.2).

3.3.1. EU-US Agreement on Mutual Legal Assistance

3.3.1.1. Exchange of Personal Data

A key provision in the EU-US Mutual Legal Assistance Agreement (EU-US MLA) is Article 4, which allows for the exchange of a wide range of everyday information about financial transactions.[158] As the House of Lords Select Committee on the European Union has noted, **the terms of Article 4 "remain broad and the provision as drafted could extend to a wide range of information about legitimate everyday transactions** of, as the [UK] Government admitted, 'innocent third parties'."[159]

3.3.1.2. Assistance to administrative authorities

Another important provision of the EU-US MLA is Article 8. It aims at extending its scope by allowing mutual legal assistance to administrative authorities. According to Article 8(1), **mutual legal assistance must also be afforded to a national administrative authority**, investigating conduct with a view to a criminal prosecution of the conduct, or referral of the conduct to criminal investigation or prosecution authorities, pursuant to its specific administrative or regulatory authority to undertake such investigation. Mutual legal assistance may also be afforded to other

---

[157] V. Mitsilegas (2012), "The Area of Freedom, Security and Justice from Amsterdam to Lisbon. Challenges of Implementation, Constitutionality and Fundamental Rights", General Report, in J. Laffranque (ed.), The Area of Freedom, Security and Justice, Including Information Society Issues. Reports of the XXV FIDE Congress, Tallinn, Vol. 3, pp. 21-142. V. Mitsilegas (2012), "The Limits of Mutual Trust in Europe's Area of Freedom, Security and Justice. From Automatic Inter-state Cooperation to the Slow Emergence of the Individual", *Yearbook of European Law 2012*, Vol. 31, pp. 319-372.

[158] Article 4(1) reads as follows: "(a) Upon request of the requesting State, the requested State shall, in accordance with the terms of this Article, promptly ascertain if the banks located in its territory possess information on whether an identified natural or legal person suspected of or charged with a criminal offence is the holder of a bank account or accounts. The requested State shall promptly communicate the results of its enquiries to the requesting State. (b) The actions described in subparagraph (a) may also be taken for the purpose of identifying: (i) information regarding natural or legal persons convicted of or otherwise involved in a criminal offence; (ii) information in the possession of non-bank financial institutions; or (iii) financial transactions unrelated to accounts." The Agreement also contains provisions on the establishment of joint investigative teams (Article 5) and videoconference arrangements (Article 6).

[159] House of Lords Select Committee on the European Union, EU-US Agreements on Extradition and Mutual Legal Assistance, 38th Report, session 2002-03, HL Paper 153, para. 31.

administrative authorities under such circumstances. Assistance must not be available for matters in which the administrative authority anticipates that no prosecution or referral, as applicable, will take place.

According to the Explanatory note to the Agreement, the first sentence of Article 8(1) imposes an obligation to afford mutual legal assistance to requesting US federal administrative authorities and to requesting national administrative authorities of EU Member States. Under the second sentence of that paragraph mutual legal assistance may also be made available to other, that is, non-federal or local, administrative authorities. **The scope of assistance is therefore very broad**. It appears to be inconsistent with the tight demarcation of the authorities allowed to operate mutual recognition in criminal matters under EU law.

3.3.1.3. Privacy and Data Protection

In an effort to address concerns with regard to the adverse impact that its provisions may have on EU privacy and data protection standards, the EU-US Mutual Legal Assistance Agreement contains a specific provision, Article 9, entitled "Limitations on use to protect personal and other data".

The wording of Article 9 has done little, however, to address these concerns. Article 9(1) sets out the purpose of the use of information obtained in very broad terms: the requesting State may use any evidence or information obtained from the requested State for the purpose of criminal investigations and proceedings; for preventing an immediate and serious threat to its public security; for its non-criminal judicial or administrative proceedings directly related to investigations or proceedings set forth in subparagraph (a), or for which mutual legal assistance was rendered under Article 8; for any other purpose, if the information or evidence has been made public within the framework of proceedings for which they were transmitted, or in any of the situations described in subparagraphs (a), (b) and (c); and for any other purpose, only with the prior consent of the requested State. **The purpose here is so wide that it is questionable whether it meets the fundamental EU data protection principle of purpose limitation**.

Moreover, and as the House of Lords Select Committee on the European Union has also underlined, no reference is made to specific data protection instruments such as Convention 108, the Data Protection Directive and the EU Charter of Fundamental Rights.[160] Data protection is weakened further by Article 9(4), according to which a requested State may apply the use limitation provision of an applicable bilateral mutual legal assistance treaty in lieu of Article 9 of the Agreement, where doing so will result in less restriction on the use of information and evidence than provided for in this Article.

This already limited data protection framework is weakened further by Article 9(2). While its first part (Article 9(2)(a)) allows States to impose additional conditions in order to comply with a request, its second part (Article 9(2)(b)) states that **generic restrictions with respect to the legal standards of the requesting State for processing personal data**

[160] House of Lords, para. 35.

may not be imposed by the requested State as a condition under subparagraph (a) to providing evidence or information.

This is an attempt to ensure that concerns with regard to EU data protection law will not constitute a barrier to cooperation under the Mutual Legal Assistance Agreement. In order to ensure that full cooperation takes place notwithstanding these concerns, the Explanatory Note to the Agreement states:

> Article 9(2)(b) is meant to ensure that refusal of assistance on data protection grounds may be invoked only in exceptional cases…A broad, categorical, or systematic application of data protection principles by the requested State to refuse cooperation is therefore precluded. Thus, the fact the requesting and requested States have different systems of protecting the privacy of data (such as that the requesting State does not have the equivalent of a specialised data protection authority) or have different means of protecting personal data (such as that the requesting State uses means other than the process of deletion to protect the privacy or the accuracy of the personal data received by law enforcement authorities), may as such not be imposed as additional conditions under Article 9(2a).

3.3.1.4 Benchmarks and Relation to Bilateral Agreements

Article 3 of the EU-US MLA aims to clarify the relationship between the EU and its Member States as regards the application of the Agreement. Uncertainty with regard to the external action powers of the EU under the old 'Third Pillar' (comprising Justice and Home Affairs cooperation under the Maastricht Treaty) resulted in **an emphasis on the maintenance or establishment of bilateral relations between EU Member States and the US**.

Article 3(1) clarifies that the EU-US Agreement supplements, and does not replace, bilateral agreements in the field. The main innovations brought about by the Agreement (provisions on the identification of bank information, joint investigation teams, videoconferencing, expedited requests and assistance to administrative authorities) apply *in addition to* any authority already provided under bilateral treaty provisions (Article 3(1)(a)-(e), respectively), while the data protection provisions apply in place, or in the absence, of bilateral treaty provisions (Article 3(1)(f)) and the provisions on confidentiality in the absence of bilateral provisions (Article 3(1)(g)).

The bilateral dimension was also emphasised by the requirement, in addition to the signature of the Agreement by the EU, for the exchange of written instruments between each EU Member State and the US, acknowledging the application of their bilateral agreements in the light of the provisions of the EU-US Agreements (Article 3(2)). **This emphasis on the bilateral dimension does not negate, however, the EU law dimension of the obligations EU Member States have undertaken under this Agreement.**

While the EU-US MLA supplements bilateral agreements, the latter do not operate in isolation from EU law. The EU law dimension is visible throughout the MLA Agreement: the Union will coordinate Member State actions regarding their exchange of written instruments with the US setting out the

application of their relevant bilateral agreements;[161] it will ensure that the provisions of the EU agreements are applied to bilateral MLA Treaties between Member States and the US;[162] it will ensure that the provisions of the EU-US MLA are applied in the absence of a bilateral treaty;[163] and it will be engaged in consultation and review processes with the US regarding the content of the agreements.[164] Moreover, **the standards set out by the EU-US Agreement will constitute a benchmark for the conclusion of future bilateral agreements** in the field between Member States and the US (Article 14).

Underpinning Member States' bilateral relations with the US by EU law is further strengthened by the non-derogation clause of Article 13. According to this provision the Agreement is without prejudice to the invocation by the requested State of **grounds for refusal of assistance** available pursuant to a bilateral mutual legal assistance treaty, or, in the absence of a treaty, its applicable legal principles, including where execution of the request would prejudice its sovereignty, security, *ordre public* or other essential interests.

Non-compliance with fundamental rights might constitute such a ground for refusal, especially after the entry into force of the Treaty of Lisbon. **The Agreement should be interpreted consistently with the requirements of EU constitutional and human rights law,** including in particular the provisions laid out above in the scope of the EU Charter as well as consistently with the Directive on the European Investigation Order (see section 3.2.2 below).

Cooperation between Member States and the US must comply with these benchmarks and comply fully with EU law. The end of the transitional period (since December 2014) regarding the role of EU institutions (and the liberalisation of the enforcement powers enjoyed by the European Commission and the Luxembourg Court of Justice) in relation to EU criminal justice and police cooperation law further confirms that **the EU-US Agreement must be treated as a full, supranational EU agreement**.[165]

---

[161] Decision concerning the signature of the agreements, Article 2(2).

[162] Article 3(1).

[163] Article 3(3)(a).

[164] Article 11 of the Mutual Legal Assistance Agreement. Moreover, note that it is the Council on behalf of the EU which will decide on the extension of the territorial scope of the agreement (Article 3 of the Decision concerning the signature of the agreements).

[165] For an assessment of the end of the Transitional Period refer to V. Mitsilegas et al. (2014), "The End of the Transitional Period for Police and Criminal Justice Measures Adopted before the Lisbon Treaty: Who Monitors Trust in the European Justice Area?", CEPS Liberty and Security in Europe Series, Centre for European Policy Studies, Brussels.

3.3.2. The European Investigation Order

The Directive on the European Investigation Order (EIO)[166] regulates the **exchange of evidence between EU Member States in the field of criminal justice**. The Directive applies the principle of mutual recognition in the field of evidence, and is the first major instrument on mutual recognition adopted after the entry into force of the Lisbon Treaty.[167]

The Directive is of major importance with regard to its applicability. It will replace, as of 22 May 2017, the corresponding provisions applicable between Member States bound by it of the Council of Europe Mutual Legal Assistance and its protocols, the Convention implementing the Schengen Agreement and the EU Mutual Legal Assistance Convention and its Protocol.[168] The Directive will also replace the Framework Decision on the European Evidence Warrant, [169] and the relevant provisions of the Framework Decision on the mutual recognition of freezing orders.[170]

In this manner, the EIO Directive will become **the sole legal instrument regulating the exchange of evidence and mutual legal assistance between EU Member States**. The transposition deadline for Member States is also 22 May 2017.[171]

The Directive is divided into two main parts: the first part (Chapters I-III) introduces the rules underpinning the application of the principle of mutual recognition in the field of exchange of criminal evidence; the second part (Chapters IV-VI) consists of a number of specific procedural provisions covering aspects of the conduct of investigations (such as provisions on temporary transfer of evidence, hearing by videoconference, covert investigations and the interception of telecommunications).

An EIO is defined as a judicial decision which has been issued or validated by a judicial authority of a Member State (the issuing State) to have one or several specific investigative measures carried out in another Member State (the executing State) to obtain evidence in accordance with the Directive.[172] It may also be issued for obtaining evidence that is already in the possession of the competent authorities of the executing State.[173] Its

---

[166] Directive 2014/41/EU regarding the European Investigation Order in criminal matters, OJ L130, 1.5.2014, p. 1.

[167] On the application of the principle of mutual recognition in criminal matters, see V. Mitsilegas (2006), "The Constitutional Implications of Mutual Recognition in Criminal Matters in the EU", *Common Market Law Review*, Vol. 43, pp. 1277-1311; and V. Mitsilegas (2009), *EU Criminal Law*, Oxford: Hart Publishing, chapter 3.

[168] Article 34(1).

[169] Council Framework Decision 2008/978/JHA on the European evidence warrant for the purpose of obtaining objects, documents and data for use in proceedings in criminal matters, OJ L350, 30.12.2008, p.72.

[170] Council Framework Decision 2003/577/JHA of 22 July 2003 on the execution in the European Union of orders freezing property or evidence, OJ L196, 2.8.2003, p. 45, Article 34(2).

[171] Article 36(1).

[172] Article 1(1) first indent.

[173] Article 1(1) second indent.

issuing may be requested by a suspected or accused person, or by a lawyer on his behalf, within the framework of applicable defence rights in conformity with national criminal procedure.[174] It may be issued:

> (a) With respect to criminal proceedings that are brought by, or that may be brought before, a judicial authority in respect of a criminal offence under the national law of the issuing State;
>
> (b) In proceedings brought by administrative authorities in respect of acts which are punishable under the national law of the issuing State by virtue of being infringements of the rules of law and where the decision may give rise to proceedings before a court having jurisdiction, in particular, in criminal matters;
>
> (c) In proceedings brought by judicial authorities in respect of acts which are punishable under the national law of the issuing State by virtue of being infringements of the rules of law, and, where the decision may give rise to proceedings before a court having jurisdiction, in particular, in criminal matters; and
>
> (d) In connection with proceedings referred to in points (a), (b) and (c) which relate to offences or infringements for which a legal person may be held liable or punished in the issuing State.[175]

The term ***"court having jurisdiction in particular in criminal matters"*** has been granted an autonomous meaning by the CJEU for the purposes of the application of the principle of mutual recognition in criminal matters. As mentioned in section 2 above, the Treaties do not provide a definition of what is a court for the purposes of EU law. The Luxembourg Court of Justice has examined the definition of this term in the case of *Baláz.*[176] It did so within the meaning of Article 1(a)(iii) of the Framework Decision on the mutual recognition of financial penalties.[177]

The first step was **to define the term "court"** contained in Article 1(a)(iii) of the Framework Decision. The Court of Justice did so by relying on the criteria it had previously developed for determining whether a referring body is a "court or tribunal" for the purposes of Article 267 TFEU. To that end, the Court reiterated the need to take into account a number of factors, such as whether the body is established by law, whether it is permanent, whether its jurisdiction is compulsory, whether its procedure is *inter partes*, **whether it applies rules of law and whether it is independent**.[178]

The second step was **to define the concept of "*having jurisdiction in criminal matters*".** The Court found that in order to ensure that the Framework Decision is effective, it is appropriate to rely on an interpretation of the words "having jurisdiction in particular in criminal matters" in which the classification of offences by the Member States is not conclusive.[179] To that end, the court having jurisdiction within the meaning of Article 1(a)(iii)

---

[174] Article 1(3).

[175] Article 4.

[176] CJEU, C-60/12, Baláz, 14 November 2013.

[177] Reference FD financial penalties.

[178] Ibid., para. 32.

[179] Ibid., para. 35.

of the Framework Decision must apply a procedure which satisfies the essential characteristics of criminal procedure, without, however, it being necessary for that court to have jurisdiction in criminal matters alone.[180] In order to determine whether a court can be regarded as a court having jurisdiction in particular in criminal matters, within the meaning of the Framework Decision, an overall assessment of a number of objective factors that characterise that body and its operation has to be carried out.[181]

The Directive states expressly that **Member States must execute the EIO on the basis of the principle of mutual recognition.**[182] In principle, the executing authority must recognise an EIO **without any further formality** being required, and ensure its execution, in the same way and under the same modalities as if the investigative measure concerned had been ordered by an authority of the executing State.[183]

The decision on the recognition or execution must be taken and the investigative measure must be carried out with the same celerity and priority as for a similar domestic case and, in any case, within the time limits provided in the Directive.[184] The decision on the recognition or execution of a EIO must be taken in principle no later than 30 days from the receipt of the Order by the competent executing authority.[185] The deadline for the executing authority to carry out the investigative measures covered by the order is a maximum of 90 days.[186] Both deadlines can be extended by a maximum of 30 days if recognition or execution is not practicable within the time limit set out in a specific case.[187]

The Directive thus introduces a system of mutual recognition based on a minimum of formality, and speed. However, there are a number of safeguards set out in the Directive which temper the automaticity in the execution of EIOs. The considerable legal diversity as regards national legislation on evidence, coupled with the potentially far-reaching consequences of mutual recognition in the field of evidence for national constitutional traditions and the protection of fundamental rights, have led to the inclusion in the text of the Directive of **a number of provisions aiming to prevent *automatic* mutual recognition**. These provisions concern in particular: the possibility of legal adaptation in the execution of an EIO; the introduction of a proportionality test; and the introduction of a specific ground for refusal to execute on fundamental rights grounds.

---

[180] Ibid., para. 36.

[181] Ibid., para. 37. For an analysis, see V. Mitsilegas (forthcoming), "Managing Legal Diversity in Europe's Area of Criminal Justice: The Role of Autonomous Concepts", in R. Colson and S. Field (eds), *EU Criminal Justice and the Challenges of Legal Diversity. Towards A Socio-Legal Approach to EU Criminal Policy*, Cambridge: Cambridge University Press.

[182] Article 1(2).

[183] Article 9(1).

[184] Article 12(1).

[185] Article 12 (3).

[186] Article 12(4).

[187] Article 12(5).

3.3.2.1. Legal Adaptation

The Directive provides a series of **safeguards with regard to the respect of the legal and constitutional system of the executing Member State**. Most notably:

- the executing authority must comply with the formalities and procedures expressly indicated by the issuing authority provided that these are not contrary to the fundamental principles of law of the executing State;[188]
- the executing authority must have recourse to an investigative measure other than that provided for in the Order where the investigative measure does not exist under the law of the executing State or the investigative measure would not be available in a similar domestic case;[189]
- the executing authority may also have recourse to an investigative measure other than that indicated in the European Investigation Order where the investigative measure selected by the executing authority would achieve the same result by less intrusive means;[190] and
- the executing authority may refuse to recognise and execute an EIO where the requirement of the respect of dual criminality has not been met for certain categories of offences;[191] and the executing authority may refuse to recognise and execute an EIO when the latter has been issued in proceedings brought by administrative or judicial authorities referred to in Article 4(b) and (c) of the Directive and the investigative measure would not be authorised under the law of the executing State in a similar domestic case.[192]

The Directive further calls for **the applicability of legal remedies equivalent to those applicable in a similar domestic case** to the investigative measures indicated in the EIO.[193]

In addition to the safeguards provided in relation to the law of the executing Member State, the Directive has included **a key safeguard as regards the integrity of the law of the issuing State**. The Directive states clearly that the issuing authority may only issue an EIO where the investigative measures indicated therein could have been ordered **under the same conditions** in a similar domestic case.[194] This provision has been included **to avoid instances where Member States use the EIO to 'fish' for evidence** and obtain evidence abroad which they are not able to obtain under their own domestic legal and constitutional procedures.

---

[188] Article 9(2).

[189] Article 10(1), but see the exceptions in Article 10(2).

[190] Article 10(3).

[191] Article 11(1)(g).

[192] Article 11(1)(c).

[193] See Article 14(1), and see para. 4 on time limits and para. 6 on suspensive effect.

[194] Article 6(1)(b).

3.3.2.2. Proportionality

A debate which has arisen in the context of the implementation of the Framework Decision on the European Arrest Warrant (EAW)[195] concerns the question of **whether the operation of mutual recognition in criminal matters should be subject to a proportionality test.** And, if so, whether this test should be conducted by the issuing or by the executing authority, or by both.

Proportionality concerns have arisen from allegations that national authorities have been issuing EAWs for trivial offences.[196] This was deemed to have an adverse effect on the efficiency of the domestic criminal justice system of the executing Member State, as the system was inundated with large numbers of requests resulting in high costs and delays, as well as an adverse effect on the fundamental rights of affected individuals.[197]

The use of the proportionality test in EAW proceedings was examined by Advocate General (AG) Sharpston in her Opinion in *Radu.*[198] While finding that the issue was not of direct relevance to that case, the AG discussed the tension between Warrants issued for perceived trivial offences on the one hand and the principle of proportionality on the other as follows:

> I would add one thing. At the hearing, counsel for Germany used the example of a stolen goose. If that Member State were asked to execute a European arrest warrant in respect of that crime where the sentence passed in the issuing Member State was one of six years, she thought that execution of the warrant would be refused. She considered that such a refusal would be justifiable on the basis of the doctrine of proportionality and referred the Court to Article 49(3) of the Charter, according to which 'the severity of penalties must not be disproportionate to the criminal offence'. This Court has yet to rule on the interpretation of that article. In the context of the Convention, the Court of Human Rights has held that while, in principle, matters of appropriate sentencing largely fall outside the scope of the Convention, a sentence which is 'grossly disproportionate' could amount to ill-treatment contrary to Article 3 but that it is only on 'rare and unique occasions' that the test will be met. It would be interesting to speculate as to the interpretation to be given to Article 49(3) of the Charter having regard to the interpretation given by the Court of Human Rights of the provisions of Article 3 of the Convention.[199]

---

[195] Council of the EU (2002), Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States, 2002/584/JHA, Official Journal L 190, 18.7.2002.

[196] For a detailed examination see S. Carrera et al. (2013), "Europe's Most Wanted? Recalibrating Trust in the European Arrest Warrant System", CEPS Liberty and Security in Europe Series, Centre for European Policy Studies, Brussels.

[197] For the debate in the UK, see Sir Scott Baker, Extradition Review; Joint Committee on Human Rights, The Human Rights Implications of UK Extradition Policy, Fifteenth Report, session 2010-12, pp. 40-3.

[198] Opinion of Advocate General Sharpston delivered on 18 October 2012, Case C-396/11 Radu.

[199] Para. 103.

The CJEU did not engage with the proportionality argument in *Radu.* However, the issue has surfaced in domestic law, with the United Kingdom recently amending the Extradition Act 2003 to expressly include proportionality as a ground for refusal to recognise and execute a EAW.[200]

The EU legislator has followed a different approach in the EIO Directive, by **introducing a proportionality test but reserving it for the issuing authority**. According to Article 6(1)(a) of the Directive, the issuing authority may only issue an EIO **where the issuing of the latter is necessary and proportionate**. This provision, coupled with the safeguard mentioned above that the issuing authority may only issue an Order where the investigative measures indicated in the EIO could have been ordered under the same conditions in a similar domestic case (Article 6(1)(b)) places clear limits on the powers of issuing authorities to abuse the EIO system.

3.3.2.3. Fundamental Rights

A central question in the development of the application of the principle of mutual recognition in criminal matters has been **whether the relevant instruments should include an express ground for refusal to recognise and execute a judicial decision on fundamental rights grounds**.

In the pre-Lisbon Treaty, EU Third Pillar legal framework on mutual recognition in judicial cooperation in criminal matters, the answer to this question has been negative. While mutual recognition instruments contained references to the respect of fundamental rights, **they did not include a specific ground for refusal in this regard**. It was felt that including a fundamental rights ground for refusal would limit unduly mutual recognition and would disregard the mutual trust underpinning the system of mutual recognition among EU Member States, all signatories to the ECHR and bound by the EU Charter of Fundamental Rights.

The EIO Directive marks a remarkable shift in this regard. While it contains a general clause proclaiming respect for fundamental rights,[201] **the Directive also contains for the first time an express ground for refusal on fundamental rights grounds**. According to Article 11(1)(f) of the Directive, the executing authority may refuse to recognise or execute an EIO where there are substantial grounds to believe that the execution of the investigative measure indicated in the Order would be incompatible with the executing State's obligations in accordance with Article 6 TEU and the Charter. **This is a major legal development**, which sets out expressly the fundamental rights parameters of the operation of the mutual recognition principle.

---

[200] In March 2014, section 157 of the Anti-Social Behaviour, Crime and Policing Act 2014, introduced proportionality as a ground for refusing to surrender an individual in section 21A of the Extradition Act 2003.

[201] According to Article 1(4), the Directive will not have the effect of modifying the obligation to respect the fundamental rights and legal principles as enshrined in Article 6 of the TEU, including the rights of the defence of persons subject to criminal proceedings, and any obligations incumbent on judicial authorities in this respect will remain unaffected.

The creation of an Area of Freedom, Security and Justice (AFSJ) within the Union is based on mutual confidence and a presumption of compliance by other Member States with Union law and, in particular, with fundamental rights. However, that presumption is rebuttable.

Consequently, if there are substantial grounds for believing that the execution of an investigative measure indicated in the EIO would result in a breach of a fundamental right of the person concerned and that the executing State would disregard its obligations concerning the protection of fundamental rights recognised in the EU Charter, the execution of the EIO should be refused.[202] This provision is important in confirming that **the presumption that all EU Member States comply with fundamental rights at all instances is rebuttable**, and in thus setting limits to blind mutual trust among States by stressing the requirement for executing authorities to examine the impact of the execution of the EIO on the affected individual.[203]

3.3.2.4. The European Investigation Order as a Benchmark for External Action

The EIO Directive is a significant legal development in the field of judicial cooperation between EU Member States and in the field of the development of the application of the principle of mutual recognition in criminal matters more broadly. The Directive reflects a constitutional settlement between Member States, by setting out clear limits and parameters to the operation of mutual recognition.

As described above, **applicable limits take the form of safeguards of the internal legal and constitutional order of the executing Member State; safeguards of the internal legal and constitutional order of the issuing Member States; proportionality safeguards; and fundamental rights safeguards. To these provisions should be added the judicialisation of mutual legal assistance**, as reflected by the definition of the authorities competent to participate in the system by the Directive and the CJEU.

The provisions of the EIO Directive constitute significant advances in the law of mutual recognition and **constitute benchmarks for EU internal and external action in the field**. Member States are duty-bound to comply with the Directive not only when they implement it under domestic law, **but also in their bilateral dealings with third countries**, especially in view of the Union's powers to conclude international agreements in the field using Article 82(1) TFEU. The Directive also acts as a benchmark for EU external action in the field, something that includes existing international agreements such as the EU-US Agreement on Mutual Legal Assistance.

---

[202] Preamble, Recital (19).

[203] V. Mitsilegas (2012), "The Limits of Mutual Trust in Europe's Area of Freedom, Security and Justice. From Automatic Inter-state Cooperation to the Slow Emergence of the Individual", *Yearbook of European Law 2012*, Vol. 31, pp. 319-372.

3.4. Cybercrime

KEY FINDINGS

- The EU has exercised legal competence in the domain of cybercrime through the adoption of the EU Directive 2013/40 on attacks against information systems, which needs to be transposed by EU Member States by September 2015.
- The Directive adopts the key definitions provided by the Council of Europe Budapest Convention on Cybercrime, and introduces important innovations concerning the use of substantive criminal law and the types of criminal offences.

Concern about cybercrime has been an adjunct to the meteoric development of information technologies. As the evolution of telecommunications technology has been embraced by individuals and businesses around the world, concerns about the protection of the vast amounts of data which are transferred has become a preoccupation of governments. The EU has had its own legal instrument on cybercrime since 2013, after the adoption of the **EU Directive 2013/40 on attacks against information systems**.

This Directive, adopted on 12 August 2013, replaced a Council Framework Decision (2005/222/JHA) which the entry into force of the Lisbon Treaty made necessary (because of the collapsing of the 'Pillars'). It entered into force 20 days after publication in the Official Journal (14 August 2013) and Member States are required to transpose the directive into national law at the latest by 4 September 2015. The legal basis is Article 83(1) TFEU.

The Framework Decision had responded to the objective of **improving cooperation between judicial and other competent authorities through the approximation of rules of Member State criminal law** relating to attacks against information systems, illegal system interference and illegal data interference. Judicial and other competent authorities include police and other specialised law enforcement services. It followed closely the main lines of the Council of Europe Budapest Convention on Cybercrime, **particularly in adopting the key definitions of the convention**.[204] The EU has not signed or ratified the Council of Europe Convention.

[204] The objective of the Budapest Convention is threefold: harmonising criminal substantive law elements of the offences and connected provisions of cybercrime; requiring the provision of domestic criminal procedural law powers necessary for the investigation and prosecution of the offences; and establishing a system for international cooperation. There are nine offences under the Convention: illegal access; illegal interception; data interference; system interference; misuse of devices; computer-related forgery; computer-related fraud; offences related to child pornography; and offences relating to copyright and related rights. Under the procedural law issues contained in the second chapter of the convention, the scope is widened. The issues here include any offence committed by means of a computer system or the evidence of which is in electronic form. The procedural powers include: expedited preservation of stored data; expedited preservation and partial disclosure of traffic data; production order; search and seizure of computer data;

The Directive retained the main elements of the Framework Decision but added **some innovations**. First, regarding substantive criminal law, it provides for penalties regarding the production, sale, procurement for use, import or distribution of, or otherwise making available, devices or tools used for the commission of the offences. It makes provision for aggravating circumstances including large-scale attacks and attacks where by reason of the concealment of the real identity of the perpetrator the rightful identity owner is prejudiced. A new criminal offence of illegal interception is included in the Directive. There is a strengthening of EU criminal justice cooperation with additional obligations on providing assistance and the production of statistics.

The criminal offences include illegal access to information systems, illegal systems interference and illegal interference. There is an element of flexibility regarding the duty to prosecute which allows Member States to criminalise only *"cases which are not minor"*. The exercise of EU legal competence in the field of cybercrime through the formal adoption of this Directive **limits the scope of action by EU Member States in the framework of the Council of Europe** Cybercrime Convention Committee (T-CY) (see section 4 below).

real-time collection of traffic data; interception of content data. There are provisions which deal with jurisdiction.

SECTION 4. CHALLENGES TO RULE OF LAW AND FUNDAMENTAL RIGHTS

KEY FINDINGS

Third-country access to data outside established legal channels of mediated assistance (MLAs) poses four legal and rule-of-law challenges:

First, the *jurisdiction challenge*:

It stands in a difficult relationship with the state territorial concept of jurisdiction. In criminal justice the notion of jurisdiction requires the conclusion of international agreements (MLAs) to handle the conflicts of law. Third-country unmediated access to data unlawfully bypasses existing legally binding channels. The resulting picture is one of legal insecurity and mistrust.

The European concept of jurisdiction in the field of human rights is foreign in the US. For all EU Member States the final word on their legal obligations is not in their constitutions. They must comply with the ECHR and supranational set of rule-of-law and fundamental rights provisions in the EU legal system.

Second, the *lawfulness and 'venue-shopping' challenge*:

These practices fail to pass the lawfulness test. Some security actors are using regional fora (venue shopping) to agree on new rules which would put at risk EU standards by legalising unilateral law enforcement access by third countries to data held by private sector actors.

Discussions such as those in the CoE on cybercrime and transborder access to electronic data pose serious challenges from the perspective of EU law.

Third, the *challenge of alleged inefficiency*:

Arguments alleging that MLA agreement models are inefficient are not substantiated by the available evidence or by statistics on their uses and practical operability.

Current obstacles affecting MLA processes can be overcome by bilateral case consultations, day-to-day contacts, stronger political commitments, more effective use of existing tools and sound financial, technological and human resources investment in their implementation.

Fourth, the *privacy and data protection challenge*:

Third-country access to data outside MLA agreements is contrary to EU data protection *acquis*. There are major dissimilarities between the EU and the US as regards data protection, not least the lack of effective judicial protection provided to EU citizens in US territory for privacy violations. This makes it difficult for EU institutions and Member States to ensure the safeguarding of EU fundamental rights and the benchmarks developed by the CJEU in the Digital Rights Ireland ruling in transatlantic operating frameworks of cooperation in the domains of law enforcement and criminal justice.

What are the legal and rule-of-law challenges raised by unmediated models of access to data by third-country authorities? This section examines the nature and scope of these challenges. Particular attention is first paid to the negative consequences of foreign authorities' access to data held by private companies under EU jurisdiction from the perspective of jurisdiction, territoriality and conflicts of law (section 4.1). A second issue of concern relates to lawfulness and venue shopping, in particular the inherent tensions raised between the promotion of unmediated models in regional venues such as the Council of Europe and the fact that the EU has already exercised legal competence in the same domains (section 4.2). A third challenge relates to claims of ineffectiveness of MLA mediated models of access to data. Section 4.3 critically reviews those claims in light of existing evidence and tests their adequacy and limitations. Finally, section 4.4 points out the privacy and data protection challenges emerging from unmediated practices from the perspective of EU data protection *acquis*.

4.1. Jurisdiction

Jurisdiction as a legal term means the reach of the law of one State over acts and individuals and thus entails responsibility for regulation. It is a way of speaking about **how and over whom what law applies**.[205] Jurisdiction is currently first and foremost a **State territorial concept**, and there is general consensus on the principle that within the territory of a sovereign State, the laws of that State apply.[206]

As various legal actors become involved in cross-border activities, the question of jurisdiction becomes increasingly complex. In any case, jurisdiction is not a single legal concept nor does it have a single coherent meaning across sovereign States. It may be interpreted very differently depending on the State involved (including as interpreted by the national courts). Jurisdiction also varies dramatically depending on the field of law under consideration.

[205] J.A. Colangelo (2014), "What is Extraterritorial Jurisdiction?", *Cornell Law Review*, 99, p. 121.

[206] The best known exception to the territorial jurisdiction rule is that contained in the Vienna Convention on Diplomatic Relations 1961, which provides for the inviolability of embassy premises and the protection of accredited diplomats from national jurisdiction in the State where they are posted.

In respect of transnational law enforcement access to data, two very different fields of jurisdiction come into contact with one another: **jurisdiction in criminal law and jurisdiction in human rights and EU fundamental rights law**. The first thing to note is that there are wide divergences between EU Member States among themselves,[207] let alone between EU States and the US, on the meaning and application of jurisdiction in criminal justice.[208]

In the domain of criminal justice, the first principle is that States may seek to exercise jurisdiction but they may or may not be successful depending on what approach the other State(s) involved takes. In the absence of international agreements on criminal justice there is no certainty that States will agree to jurisdictional claims of other States which require the first State to do or refrain from doing something.

Where the problem relates to "evidence", **the country seeking to prosecute will need to have an agreement on mutual legal assistance (MLA) with the country where the evidence needs to be collected**. Otherwise, any effort by the police in the second country to collect the evidence may be illegal as unrelated to the prosecution of criminal offences in the territory.

Neither police nor prosecutors nor courts can act to assist a prosecution elsewhere unless permitted by law. Though rare, it does happen that more than one country wants to prosecute the same person (often for the same offence). Once again there will need to be rules and agreements on how this should happen and on the basis of which principles – for instance, the UK and the US have an agreement on handling concurrent jurisdiction.

Here, however, a competing system of jurisdiction enters the field – that of European human rights and EU fundamental rights law. An illustrative example relates to the principle of *ne bis in idem,* which is inscribed in both the European Convention on Human Rights (Article 4 Protocol 7)[209] and the EU's Charter of Fundamental Rights (Article 50).[210] This competing system of jurisdiction is particularly compelling in the EU and is driven by completely different principles and according to entirely separate rules from criminal justice competence.

The European concept of jurisdiction in the area of human rights/fundamental rights is rather foreign to US jurists and law enforcement authorities. It has no US counterpart as it is an expression of a very strong supranational normative and legally constraining framework within which States are obliged to act or refrain from acting.

While as in the US, all EU and Council of Europe States have constitutions, these constitutions are not the final word on their 'constitutional'

---

[207] L. Reydams (2000), "Universal Criminal Jurisdiction: The Belgian State of Affairs", *Criminal Law Forum*, Vol. 11. No. 2.

[208] P. Alldridge (2012), "UK Bribery Act: The Caffeinated Younger Sibling of the FCPA", *Ohio St. LJ*, 73, p. 1181.

[209] An example of the principle at work can be found in PIRTTIMÄKI v. FINLAND 20 May 2014 European Court of Human Rights.

[210] For an example of the principle at work in the EU context see Spasic C-129/14 PPU, 27 May 2014.

obligations. They must also comply with both the European Convention on Human Rights (Article 6 TEU) and the EU Charter of Fundamental Rights if they are EU Member States (Article 6 TEU). The European Convention on Human Rights is interpreted by the European Court of Human Rights based in Strasbourg and the EU Charter of Fundamental Rights is interpreted by the Court of Justice of the European Union based in Luxembourg.

By and large the two courts try to avoid conflict.[211] So far, the CJEU has not had to delve into the intricacies of jurisdiction beyond the EU – though it has been very much taken up with intra-EU jurisdiction issues. On the other hand, the ECtHR has developed a very dynamic interpretation of the jurisdiction of the ECHR over the past 20 years.

For the purposes of this study, what is critical in this jurisprudence is the fact that **the ECHR right to respect for privacy** (Article 8) **is governed by a completely different set of rules on jurisdiction than criminal law** (regional, national or international). Agreements among States on jurisdiction in criminal matters cannot constrain the application of the Article 8 right to respect for privacy on actors within Council of Europe States. **It is just not possible to modify European human rights obligations through bilateral or multilateral agreements**. Only an amendment to the ECHR itself can have that effect.

Jurisdiction for the purposes of the ECHR is very wide indeed and is integrally connected with the principle of State control. So long as a State is in control of the territory or actions which take place, it is likely also to have jurisdiction over them for the purposes of determining human rights responsibility. The State is equally responsible for human rights violations by virtue of its failure to regulate the activities of private sector actors under its jurisdiction.[212]

The fact that different jurisdictions offer different types and degrees of privacy protection on the web only complicates matters. Some providers have been publicising the location of their services in a strong data protection jurisdiction in order to attract customers concerned about their privacy.[213] Others suggest that their use of the web is more limited in territorial scope. As the research of Binns et al.[214] indicates, as regards available data for the UK only, 90% of data collection was not transferred outside the European Economic Area. As regards jurisdiction, **the duty to ensure respect for privacy in accordance with Article 8 ECHR and**

---

[211] C. Costello (2006), "The Bosphorus ruling of the European Court of Human Rights: Fundamental rights and blurred boundaries in Europe", *Human Rights Law Review*, 6.1, pp. 87-130.

[212] In Tatar v. Romania, 27 January 2009, the ECtHR found the State in violation of Article 8 (the right to respect for private and family life) as a result of the actions of a private company. The ECtHR held that the authorities had failed in their duty to assess, to a satisfactory degree, the risk that the company's activities might entail, and to take suitable measures in order to protect the rights of those concerned.

[213] R. D. Binns, D. Millard, and L. Harris (2014), "Data havens, or privacy sans frontières?: a study of international personal data transfers", Proceedings of the 2014 ACM Conference on Web Science, ACM.

[214] Ibid.

Article 7 Charter rests with the State Parties (47 of the Council of Europe and 28 of the European Union).

If these States allow arbitrary or unjustified interference with individuals' privacy either through a failure to legislate or control adequately the activities of companies on their territory, then **they risk being in violation of Article 8 ECHR and Article 7 Charter**. If State authorities actively engage in measures which interfere with the right to respect for privacy whether on their own territory or in places where they exercise control even temporarily (e.g. cables in international waters), then the violation will be within their jurisdiction and they will need to justify the interference to the usual high standard which the ECtHR and CJEU apply.[215]

The central challenge for the EU in light of the described competing models of transnational law enforcement access to data is, undoubtedly, to preserve the rule of law in unmediated access to data practices. 'Unmediated' access practices and, in particular, those allowing for 'unmediated' access by authorities from countries that are not members of the Council of Europe, directly affect the possibility for individuals to seek judicial remedies in relation to compliance with their fundamental rights.

Moreover, even though, in principle, transnational law enforcement access to data concerns specific data requests, as opposed to mass surveillance, **the line between a specific request of data and mass surveillance might be difficult to determine in practice**. In this sense, bulk data requests (for instance, referring generally to all the emails of the users of some Internet services) can affect large quantities of email accounts and users.

It becomes thus crucial to **strictly circumscribe the possibility for any 'unmediated' access to data from taking place**, especially to the benefit of a third country such as the US, which is not only not a member of the Council of Europe but has also not ratified the Council of Europe's Convention 108. This, however, can be rendered especially difficult by the activities of EU Member States outside the EU framework – bilaterally or through the Council of Europe. It is then particularly important to take into account **the competence of the EU in these matters**.

Unmediated access by US authorities to data controlled by a private company falling under EU jurisdiction constitutes a fundamental challenge to both the notion of jurisdiction in criminal law and in human rights and EU fundamental rights law. It directly and transparently bypasses the use the existing legally binding channels foreseen in the scope of EU-US MLA agreements.

By doing so **the required 'consent' by the requested EU Member States** (and their designated central authority, usually the Ministry of Justice) **and the supervision by independent judicial authorities are circumvented**. The resulting picture is one where **conflicts of law emerge and legal uncertainty, mistrust and insecurity** for the parties involved take over.

---

[215] Copeland v. UK 3 April 2007. Just on this point it is worth recalling that the right to respect for privacy applies equally to emails and letters.

4.2. Lawfulness and Venue Shopping

The legal instruments analysed in section 3 above provide a transparent picture of the ways in which the EU has progressively exercised and extended competence over fields with direct relevance when assessing third-country access to data for law enforcement purposes. Some of these instruments provide clear benchmarks and standards which delimit the discretion and room for manoeuvre of EU Member States and law enforcement/criminal justice authorities' access to electronic data for purposes of fighting criminality.

EU institutions have sometimes publicly expressed a clear position on these matters. A 2014 letter from former Commissioner for Justice Viviane Reding,[216] in response to parliamentary questions posed by the MEP Sophie in 't Veld, expressed the European Commission's concerns over **the extraterritorial application of foreign laws which could be in breach of international law, and over companies bound by EU data protection law 'caught in the middle' of a conflict of laws**. The letter also stated that it had raised this issue with the US government on a number of occasions and that it

> …remains of the view that where governments need to request personal data held by private companies and located in the EU, requests should not be directly addressed to the companies **but should proceed via agreed formal channels of co-operation between public authorities, such as the mutual legal assistance agreements or sectorial EU-US agreements authorising such transfers**. In the context of the negotiations on the umbrella agreement on data protection in the area of law enforcement and judicial cooperation, the Commission has asked the US to undertake commitments in that regard, in order to avoid these potential conflicts of laws. In parallel, the EU institutions should continue working towards the swift adoption of the EU data protection reform, in order to ensure that personal data is effectively and comprehensively protected [emphasis added].

The new Commissioner for Justice, Věra Jourová, replied also in 2014 to a question introduced by the MEP Carlos Coelho,[217] who inquired, first, whether the European Commission considered that enforcement of this order constitutes a breach of the current EU legal framework on data protection and/or a breach of the fundamental right to privacy, and, second, whether the Commission was planning to intervene in any way. In answer to these questions, Commissioner Jourová stated:

> The Commission's view is that personal data held by private companies in the EU should not, in principle, be directly accessed by or transferred to foreign enforcement authorities outside of formal channels of cooperation, such as for example the Mutual Legal Assistance treaties (MLATs). The Commission has brought this point

---

[216] Letter from Viviane Reding to Sophie in 't Veld, Member of the European Parliament (24 June 2014), http://www.nu.nl/files/nutech/Scan-Ares-MEP-in%27t-Veld-.pdf.

[217] http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+WQ+E-2014-010602+0+DOC+XML+V0//EN.

> to the attention of the US authorities on several occasions and is resolute to further insist on finding a solution to this question.

EU institutions have also raised the issue of the "*the need to clarify that personal data held by private entities in the territory of the other party will not be accessed by law enforcement agencies outside of legally authorized channels"* in the context of EU-US discussions. In this sense, for instance, a Joint Press Statement following a EU-US Justice and Home Affairs Ministerial Meeting in Washington, D.C., in November 2013[218] pointed out that during the meeting there had been "*discussions"* on that subject.

In the **Riga Statement**[219] **on enhancing transatlantic cooperation in the area of justice, freedom and security** of 3 June 2015 the EU and the US expressed their commitment to

> Enhance the implementation of the U.S.-EU Mutual Legal Assistance Agreement (including in relation to transmission of financial information), conclude its review as foreseen by the Agreement and conduct workshops (including through Eurojust) to discuss such issues with national competent authorities.

The European Commission is indeed currently reviewing the MLA agreement. On that same occasion Commissioner Jourová emphasised:

> The European Commission has recently adopted the European Agenda on Security. It stresses the need for a criminal justice approach to fighting organised crime and terrorism covering investigation and prosecution, recruitment, training, and financing. The Agenda calls for reinforced criminal justice cooperation, both inside the EU and with our close partners, such as the United States. And this cooperation must take place in full respect of fundamental rights and values, including the protection of personal data. We therefore also discussed the need for effective data protection rules.[220]

These high-level political commitments to the implementation of the EU-US MLA stand in contrast with developments and discussions taking place in

---

[218] Joint Press Statement following a EU-US-Justice and Home Affairs Ministerial Meeting of 18 November 2013 in Washington, D.C., http://europa.eu/rapid/press-release_MEMO-13-1010_en.htm.

[219] Available at https://eu2015.lv/images/Kalendars/IeM/Riga_Statement_EU_US_Ministers.pdf. See also https://eu2015.lv/news/media-releases/2003-eu-us-justice-and-home-affairs-meeting-endorses-riga-statement-for-transatlantic-cooperation-in-the-area-of-freedom-security-and-justice.

[220] European Commission, Speech, Press speaking points of Commissioner Jourová at the EU-US-Justice and Home Affairs Ministerial Meeting in Riga, available at http://europa.eu/rapid/press-release_SPEECH-15-5112_en.htm. See also European Commission, European Agenda on Security, COM(2015)185 final, 28.4.2015, which states, "Mutual legal assistance (MLA) agreements with third countries (United States, Japan) are key instruments for international judicial cooperation, and the Commission will assess whether it is necessary to develop other bilateral or multilateral agreements with key third countries", and "Eurojust can also be a great help for complex mutual legal assistance requests with countries outside the EU, especially with the network of the Eurojust contact points."

the context of **the Council of Europe Cybercrime Convention Committee (T-CY), which has been seen as an example of 'venue shopping'**. In a field of law where clear EU-level transnational rule-of-law standards exist, some EU Member States and security professionals are using these regional meetings to agree on new rules which would lower and even put at risk those standards by legalising unilateral and direct law enforcement access to data held by private sector actors under EU jurisdiction.

The dilemmas posed by these discussions from the perspective of lawfulness has been pointed out by the European Parliament in relation to concerns on the work conducted by the Cybercrime Convention Committee (T-CY) of the Council of Europe on transborder access to data and the initiative to conclude a new additional Protocol to the Convention on the matter which would substantially amend the current Article 32.b of the Budapest Convention.

The European Parliament's Mass Surveillance Enquiry resulted in the 21 February 2014 Moraes Report on the US NSA surveillance programme and surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and transatlantic cooperation on JHA.[221] The Moraes Report stated in paragraph 32:

> Stresses its *serious concerns* in relation to the work within the Council of Europe's Cybercrime Convention Committee on the interpretation of Article 32 of the Convention on Cybercrime of 23 November 2001 on transborder access to stored computer data with consent or where publicly available, and opposes any conclusion of an additional protocol or guidance intended to broaden the scope of this provision beyond the current regime established by this Convention, which is already a major exception to the principle of territoriality because it could result in **unfettered remote access** by law enforcement authorities to servers and computers located in other jurisdictions without recourse to MLA agreements and other instruments of judicial cooperation put in place **to guarantee the fundamental rights of the individual, including data protection and due process**, and in particular Council of Europe Convention 108 [emphasis added].

In December, a Report adopted by the Council of Europe T-CY Committee acknowledged that the Moraes Report "includes strong criticism of the ongoing work of the T-CY on transborder access to data". It also referred to the exchange of views at a mini-hearing organised by the Parliament's LIBE Committee on 24 September 2014, where T-CY representatives presented their ongoing work, as "rather controversial".[222] During the mini-hearing the compliance of the proposals from the perspective of EU law was highlighted by some MEPs. **They expressed the lack of a proper legal**

---

[221] Refer to http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A7-2014-0139+0+DOC+XML+V0//EN.

[222] Council of Europe, Cybercrime Convention Committee (T-CY), Transborder access to data and jurisdiction: Options for further action by the T-CY, 3 December 2014, Strasbourg, p. 10.

basis to negotiate such a protocol because the EU had already exercised legal competence in the field of cybercrime, exchange of information and data protection.

A confidential opinion issued by the Parliament's Legal Service concluded that[223] while the work in the context of the Council of Europe is far from being complete and conclusive, the Union had exercised competence in these areas and that several pieces of EU law cover to a large extent the area dealt with by the Convention.[224] It also underlined that a risk that common EU rules would be affected is not enough, and even if there is no possible contradiction between EU rules and other potential commitments EU Member States should refrain from entering into international commitments. The Parliament's Legal Service concluded that **the EU has external competence in the area forming the subject matter of the Budapest Convention. Therefore, any future negotiation should be the competence of the European Commission**.

4.3. Inefficiency?

Arguments in favour of the operability or legalisation of remote/unmediated access to data controlled by companies under EU jurisdiction often refer to **the inefficiency of the current MLA mediated model**. The US government has expressed as one of its arguments in the Microsoft Search Warrant Case that MLA procedures would be lengthy and would not result in a prompt disclosure of the required data (see section 2.2.2 above). In the same vein, discussions in the framework of the Council of Europe Cybercrime Convention Committee (T-CY) have made similar claims when concluding that MLA processes are "inefficient in general, and with respect to obtaining electronic evidence in particular".[225]

This section critically examines **the extent to which arguments on the inefficiency are in fact well substantiated and justified on the basis of objective evidence**. What are the main issues behind the obstacles characterising the operability and implementation of MLA channels for meditated access to data in foreign jurisdictions? Can it be concluded that MLAs are inefficient in general? Special attention is paid to available information regarding the operability of the EU-US MLA agreement (section 4.3.1), and an assessment report on mutual legal assistance provisions conducted by the CoE Cybercrime Convention Committee (section 4.3.2).

---

[223] European Parliament, Legal Service, Note: LIBE – Convention of the Council of Europe on Cybercrime (CTS 185) – European Union Competence, 29.1.2015.

[224] These include, *inter alia*, through the adoption of the Directive 2013/40/EU on attacks against information systems (OJ L 218, 14.8.2013), the Council Framework Decision 2006/960/JHA on simplifying the exchange of information and intelligence between law enforcement authorities of EU Member States (OJ L 386, 29.12.2006), the Directive 2014/41 regarding the European Investigation Order in criminal matters (OJ L 130, 1.5.2014) as well as the Council Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation (OJ L 350, 30.12.2008).

[225] Council of Europe, Cybercrime Convention Committee T-CY, T-CY Assessment Report: The mutual legal assistance provisions of the Budapest Convention on Cybercrime, 3 December 2014, Strasbourg.

section 4.3.3 outlines the actual issues which need to be taken into consideration when assessing the effectiveness of MLA mediated models of access to data.

4.3.1. The EU-US MLA in Practice

Publicly available information on the practical use and implementation of the EU-US MLA agreement is lacking. A questionnaire leaked by *Statewatch* provides detailed information on its application.[226] The questionnaire was drafted in preparation for the workshop on the application of the MLA and extradition agreements between the European Union and the US organised by the EU Agency Eurojust (the European Union's Judicial Cooperation Unit) on 25-26 October 2012.[227] It provides information on the application of the EU-US MLA between 1 February 2010 and 31 August 2012.

What do the questionnaire responses tell us about **the efficiency or inefficiency in the operability of the EU-US MLA, and the existence of practical obstacles and promising practices characterising the use of the MLA procedures** in transatlantic relations?

A majority of EU Member State authorities reported **excellent cooperation in the application of MLAs with the US**. From the statistical information provided in Table 2 below, Germany, Spain, Poland, the Netherlands and the UK are at the top of list of EU Member States issuing MLA Requests to the US.[228] Finland, Cyprus, Denmark, Italy and Ireland underlined that the cooperation works very well and no legal/practical obstacles exist.[229]

Table 2. Number of MLA requests issued by EU Member States to the US 2010-12

EU Member State	MLA Requests Issued
Austria	-
Belgium	-
Bulgaria	61
Croatia	-
Cyprus	17
Czech Republic	98
Denmark	23
Estonia	24
Finland	23

[226] See http://www.statewatch.org/news/2012/nov/eu-council-eu-usa-mla-requests-14253-rev2-12.pdf.

[227] Council of the EU, 14253/2/12, Brussels, 24 October 2012.

[228] Information on number of MLA requests received from the US is lacking.

[229] Only Hungary states that in a majority of the cases the US authorities do not accomplish their MLA requests.

France	148 (110 requests for international judicial assistance issued by courts and 38 requests for investigation from the public prosecutors' offices)
Germany	471
Greece	171
Hungary	53
Ireland	79
Italy	78
Lithuania	80 (76 pre-trial and 4 in trial)
Latvia	2 (trial stage) and 27 (pre-trial stage)
Luxembourg	7
Malta	7
The Netherlands	274
Poland	294 (8 trial stage and 286 in pre-trial)
Portugal	-
Romania	37 (investigation phase on cybercrimes) and 29 (investigation of other serious offences) 100 in trial stage
Slovakia	35
Slovenia	51
Spain	315
Sweden	144
UK	256

Source: Council of the EU, 14253/2/12, Brussels, 24 October 2012.

What have been the main practical obstacles reported by Member State authorities when cooperating with the US in the scope of the Agreement? The following can be highlighted:

1. **An informal application of a 'proportionality test'**. US authorities do not execute an MLA request if financial interest is under $5,000,[230] or $10,000 in fraud causes.[231] Cases US authorities consider the cases as 'less serious' (*de minimis* or 'low priority') or in which the patrimonial loss is 'minimal' or "when the offence on which the request is based has not had serious consequences or the scope of the assistance sought is disproportionate in relation to the possible sentence imposed"[232] are

[230] Answers by Bulgaria and Poland.

[231] Answer by Lithuania.

[232] Answers by Spain, Poland, Romania, Slovenia. The response by Greece underlined a similar issue.

sometimes rejected and not duly processed, even though such grounds for refusal are not laid down in the MLA.[233]

2. A key legal obstacle underlined in the questionnaire responses is the **US 'probable cause' evidence requirement.** This requires providing a detailed statement of facts without conclusions.[234]

3. Some EU Member States alluded to **obstacles based on US laws.** A first issue relates to the First Amendment of the U.S. Constitution, which enshrines freedom of expression and prohibits the criminal prosecution of speech, where MLA requests are rarely successful. France reported such an obstacle in cases of 'public defamation or public insult'.[235] A second issue relates to obstacles when requesting a hearing of the accused or specific investigatory measures, such as taking victims' statements.[236]

4. Another practical issue underlined by the questionnaire responses was that the US does not have a **minimum retention period of electronic data**.[237]

5. **The length of time of the procedure** was also referred to as another practical obstacle.[238] This often relates to the need to translate the request, which has been reported to be critical in urgent cases such as those related to the freezing of a bank account.[239]

---

[233] Lithuania stated that few MLA requests received no reaction by US authorities.

[234] The response by Spain stated, "The problem is that, in most cases, the request is sent to the US in a pre-trial investigation, and so the Spanish judge hasn't still got very detailed information to provide". The issue was raised by Germany, which reported, "[I]t is often impossible for German authorities to demonstrate a probable connection between the evidence to be seized and the underlying offence at the time confirmation is required". German authorities highlighted that this is particularly the case in respect of email data, and stated, "German authorities have recently started approaching American providers directly with the express authorization of the US Department of Justice and with the aim of data being supplied on a voluntary basis". The Spanish authorities also mentioned a similar obstacle in requests seeking "email content information", where very detailed information needs to be provided by the judge. Lithuania, Sweden and the Czech Republic report a similar kind of obstacle related to the "probable cause" requirement. France also signalled a similar issue in respect of electronic data and requests for MLA aimed at obtaining content, and Luxembourg in cases of cybercrime.

[235] A similar issue was raised by the Czech Republic, Greece and Slovakia.

[236] Responses by Romania, Sweden, Slovenia and Slovakia. Sweden also reports, "[W]hen an investigation is on-going in both countries, it seems to be difficult to receive information from US authorities that may be used in Swedish investigation".

[237] France emphasised data retention rules depend on each US company and foreign judicial authorities lack a clear overview of these time periods. France also declared, "US companies require a minimum of factual material concerning the ongoing investigation, which can pose problems for the French authorities because of the principle of investigation secrecy in French law". Other countries, such as Lithuania, also mention the limited time of data retention as an obstacle.

[238] Answers by Malta, Luxembourg, Poland, Romania, Slovenia and Slovakia.

[239] Answer by the Czech Republic.

Despite these practical obstacles, several EU Member State authorities emphasised that **legal or practical obstacles are usually overcome through bilateral case consultations and daily contacts** between central authorities.[240] They were said to be solved/dealt with informally and via direct contact with US authorities.[241]

In light of the above, one can conclude that the questionnaire providing information on the application of the EU-US MLA between 1 February 2010 and 31 August 2012 showed that a majority of EU Member State authorities reported excellent cooperation in the application of MLAs with the US. While several practical obstacles have been highlighted, **there is no evidence substantiating the argument that the EU-US MLA is ineffective, which would properly justify bypassing its application.**

4.3.2. The Assessment by the Cybercrime Convention Committee

A similar finding can be concluded when looking at the results of an assessment of MLAs conducted by the Council of Europe Cybercrime Convention Committee T-CY.[242] The T-CY concluded, "The mutual legal assistance (MLA) process is considered inefficient in general, and with respect to obtaining electronic evidence in particular".[243] It added:

> Replies suggest that MLA is considered too complex, lengthy and resource-intensive to obtain electronic evidence, and thus often not pursued. Law enforcement authorities tend to attempt to obtain information through police-to-police cooperation to avoid MLA, even though the information thus obtained in most cases cannot be used in criminal proceedings.[244]

---

[240] E.g. the Czech Republic, Romania and the Netherlands.

[241] Answers by Denmark and Lithuania. This was also mentioned in the reply from French authorities, which states that "almost daily contact" between the relevant authorities means that "any problems likely to arise…can be anticipated or resolved in the context of what are often constructive exchanges". Malta reported that the time period to execute a request improved considerably given "the direct contact" with the U.S. Department of Justice. The UK stated that in each country there is a "Liaison Prosecutor/Legal Attaché who are responsible for facilitating the provision of MLA between the two countries", and that the UK Liaison Prosecutor had issued a guide to obtaining email/Internet data from the US which is used by UK prosecutors when drafting MLA requests and guarantees compliance with US law.

[242] Council of Europe, Cybercrime Convention Committee T-CY, T-CY Assessment Report: The mutual legal assistance provisions of the Budapest Convention on Cybercrime, 3 December 2014, Strasbourg.

[243] Council of Europe (2015), Criminal Justice Access to Data in the Cloud: Challenges, Discussion Paper prepared by the T-CY Cloud Evidence Group, 26 May 2015, Strasbourg, p. 11. It argues, "The mutual legal assistance (MLA) process is considered inefficient in general, and with respect to obtaining electronic evidence in particular. Response times to requests of six to 24 months appear to be the norm. Many requests and thus investigations are abandoned. This adversely affects the positive obligation of governments to protect society and individuals against cybercrime and other crime involving electronic evidence."

[244] It is also stated that "police-to-police cooperation for the sharing of data related to cybercrime and e-evidence is much more frequent than mutual legal assistance (the ratio seems to range from 10:1 to 50:1)". The assessment report concludes,

The assessment is based on answers/inputs to a questionnaire received between April 2013 and November 2014 by Council of Europe members. Not all EU Member States replied to the questionnaire. A key finding of the assessment is that most States were not able to provide specific statistics on 'the frequency' of MLA to stored computer data. The reasons identified for this were the increasingly decentralised MLA process, where requests are sent directly between relevant 'judicial authorities' and not only via the central authorities,[245] and that no separate statistics are kept for requests on electronic data.

The argument of 'ineffectiveness' developed in the T-CY assessment suffers, however, from a number of unanswered questions. The assessment provides no clear evidence that practical obstacles in the operability of MLAs justify concluding that the mediated model of access to data lacks efficiency. Neither is it clear how current practical hurdles can back up the argument that an "MLA is not always a realistic solution to access evidence in the loud context".[246] The question of lack of effectiveness is first challenged when looking at the level of frequency of use that the Discussion Paper and the assessment assume. They do not take duly into account the reasons why some of the MLA requests may be actually refused, which often have to do with procedures necessary to delivering justice between two jurisdictions.

In fact, and similar to the results of the Eurojust questionnaire on the EU-US MLA analysed in section 4.3.1 above, the CoE assessment points out a number of legal grounds which are often referred to when MLA requests are rejected. In particular, those referring to 'time' and the referred 'delays' (6-24 months) are often related to the lack of 'mutual recognition' between the jurisdictions at hand, the existence of 'informal grounds of refusal' (e.g. proportionality, *ne bis in idem*, etc.) or specificities of the legal systems at hand.[247]

Also surprising is the assessment's conclusion that one of the key reasons affecting the effectiveness of existing MLA frameworks is that "the Parties appear not to make full use of the opportunities offered by the Budapest Convention on Cybercrime and other agreements for the purpose of effective mutual legal assistance related to cybercrime and electronic evidence". Therefore, is the MLA system inefficient or rather do the answers to the questionnaire show the lack of willingness of relevant authorities to

---

"[T]he MLA process is considered inefficient in general, and with respect to obtaining electronic evidence in particular". See p. 123.

[245] It is said that "[m]ultiple offices may be involved in the sending or receiving of requests and in particular the execution of requests", p. 6.

[246] Ibid.

[247] See pp. 33-34 of the assessment. These are issues which come very clearly from the findings highlighted in the T-CY assessment which, when addressing problems encountered in respect of "procedure for sending/receiving requests", highlights the following issues in respect of the US: request may not meet the legal threshold or formal requirements of the requested State or request not complete or threshold/standard required too high; inadequacy of the laws to permit countries to assist others; 'probable cause' requirement. Pp. 38-39.

make proper and effective use of the existing criminal justice cooperation tools?

4.3.3. Addressing Efficiency

Within the scope of the EU-US MLA, the responses to the Eurojust questionnaire are clear: The legal and practical obstacles which were reported have been said to be overcome through direct and daily contacts/communications between relevant authorities, **in particular in relation to addressing the challenge of the duration of the procedure**.

Issues such as **lack of adequate staffing and financial resources** may be in this respect critical. While there might be important obstacles and barriers affecting the use of MLA processes, these can be overcome by bilateral case consultations, day-to-day contacts, stronger political commitments by all the parties involved on their uses and proper financial, technological and human resources investment in their implementation.

Pressures are mounting in the US to effectively address some of the current obstacles by increasing funding for US MLA processes.[248] Improving MLA technologies, including digital certification, transmission, intake and processing[249] has been suggested as a key way forward in contributing to increasing the efficiency of current procedures.

The unilateral use of 'unmediated models' of access to data by any of the parties involved profoundly **endangers the trust placed in these day-to-day working relationships** which have until present overcome practical obstacles. As highlighted in section 3.2 above, when studying the EU-US MLA, the scope of many of its provisions and exceptions is already very broad in nature. This is the case in respect of **privacy and data protection standards** in the Agreement, which are **largely weak** and subject to wide-ranging exceptions. It would be therefore difficult to argue that they constitute insurmountable barriers to criminal justice cooperation.

A key finding coming out of the questionnaire's responses and which raises a number of concerns relates to the lack of a general picture of practices regarding grounds of refusal by US authorities and EU Member States, or informal procedures or channels agreed between each EU Member State and the Department of Justice in respect of electronic data and cooperation with private sector.[250]

---

[248] http://www.itic.org/dotAsset/3/f/3f626c7e-f34d-42d6-a86b-4cf61b02ef3c.pdf.

The Department's FY 2015 Budget has requested an additional $24.1 million for significantly increasing the personnel dedicated to reviewing and executing MLAT requests as well as technological enhancements to vastly improve the way requests are prioritised, analysed and categorised. See http://www.justice.gov/sites/default/files/jmd/legacy/2014/07/13/mut-legal-assist.pdf.

[249] A. K. Woods (2015), "Data Beyond Borders: Mutual Legal Assistance in the Internet Age", Global Network Initiative.

[250] On the importance of information gathered in an 'informal' manner, see T. Markus Funk (2014), "Mutual Legal Assistance Treaties and Letters Rogatory: A

This relates to **the lack of a permanent/systematic and independent system evaluating the operability and application of the EU-US MLA**, as well as the set of bilateral agreements. There is neither a systematic statistical gathering on the actual number of MLA requests issued and received by EU Member States and the US, which adds to the obscurity and lack of transparency and accountability of the current EU-US MLA frameworks.

A key challenge of the current MLA model is not its lack of efficiency, but rather **the difficulty of ensuring consistency** of bilateral agreements/practices with general/umbrella agreement principles/rules, as well as with informal practices which have developed during the last five years as regards grounds for refusal or kinds of cooperation on questions related to evidence and investigations. To this we may add the challenge of ensuring compliance with the set of EU legal standards studies in section 3 above in a post-Lisbon Treaty landscape.

The question of 'effectiveness' very much depends on 'whose perspective' the question is raised. From the perspective of 'delivery of justice' by an independent court of law, rapidity or speed is counterproductive to the rule of law. It is no surprise that police-to-police cooperation is faster, as the rule-of-law test is absent.

4.4. Privacy and Data Protection

A key challenge posed by US authorities' access to data under EU jurisdiction is **its incompatibility with EU data protection *acquis***, and more specifically the ways in which it challenges **the European understanding or notion of 'privacy'** as developed by the ECtHR and now also enshrined in Article 7 of the EU Charter of Fundamental Rights. Safeguarding European rights against unlawful access and misuse of data in the transatlantic context requires taking into account the discrepancies between the EU and the US regimes.

EU institutions and Member States have the obligation to ensure the safeguarding of EU fundamental rights in any operating framework of transnational cooperation in the domains of law enforcement and criminal justice, including (but not limited to) privacy and data protection. In the EU legal system fundamental rights are not exclusively enjoyed by EU citizens or residents, but more generally by all natural persons. For instance, Articles 7 and 8 of the EU Charter refer to "*Anyone*", and therefore do not delimit the personal scope of application to EU citizens or nationals of EU Member States.

It is therefore necessary for the EU to ensure that any framework of international cooperation, and its implementation, ensures the protection of **the rights of EU citizens as well as any other person whose data and rights must nevertheless be protected under EU law**. [251]

Guide for Judges", Federal Judicial Centre, International Litigation Guide, pp. 1 and 23.

[251] The inclusion in the proposed General Data Protection Regulation of criteria delimiting its scope of application related to the place of residence of data subjects does not alter the basic principle derived from EU fundamental rights. Furthermore, the general reach of the EU personal data protection *acquis* has been already

Significant inconsistencies exist between the EU and US regimes in relation to personal data protection. **The US legal system and surveillance practices place non-US residents in a particularly weak position**, unlike that which is generally enjoyed by US residents. This **structural vulnerability of non-residents in the US legal system** cannot be easily solved.

The U.S. Constitution's Fourth Amendment does not protect all people, but only the individuals who have established a voluntary connection to the US as a sovereign.[252] In addition, the Fourth Amendment provides almost no protection for data stored by third parties, even though requesting data of third parties is, precisely, the way in which EU law enforcement authorities typically pursue accessing data by non-US citizens.[253] As it has been studied in section 3.2 above, the negotiations of the EU-US data protection umbrella agreement depend on progress on securing **EU citizens who are not resident in the US the right to effective judicial redress if their data has been mishandled. This issue remains open.**[254]

There is room for these discrepancies to be reduced in the future. Following the 2013 Snowden revelations there have been recent signs hinting towards **a general reinforcement of privacy protection in the US**. The U.S. Privacy and Civil Liberties Oversight Board severely criticised governmental

---

explicitly inscribed in some EU-US legal instruments. The 2010 EU-US TFTP Agreement, for instance, describes a series of "Safeguards applicable to the processing of Provided Data" that are to be provided by the U.S. Treasury Department "without discrimination, in particular on the basis of nationality or country of residence". See Article 5(1) of the EU-US TFTP Agreement.

[252] United States v. Verdugo-Urquidez, 494 U.S. 259, 271 (1990). See also, on this subject, O. S. Kerr (2010), "The Fourth Amendment and the Global Internet", *Stanford Law Review*, Vol. 62, No. 4, p. 288.

[253] In United States v. Miller (1976), the U.S. Supreme Court held indeed that there is no reasonable expectation of privacy regarding information held by a third party. 425 U.S. 435. In Smith v. Maryland (1979), this 'third party doctrine' was further reinforced as the Court held that the Fourth Amendment does not apply to transactional information associated with making phone calls. Foreign (non-US) individuals are also particularly targeted through the Foreign Intelligence Surveillance Act of 1978 (FISA). Pub. L. 95–511, 92 Stat. 1783, 50 U.S.C. ch. 36. FISA authorises the interception of real time communications when there is 'probable cause' to believe that the target of the electronic surveillance is a foreign power or agent of a foreign power, and each of the facilities or places at which electronic surveillance is directed is being used, or is about to be used by a foreign power or an agent of a foreign power.

[254] Additionally, in January 2014, U.S. President Obama signed Presidential Policy Directive 28 on Signals Intelligence Activities, and delivered an address at the Department of Justice on the steps to reform certain intelligence activities. Section 4 of Presidential Policy Directive 28 requires the intelligence community to establish policies and procedures for safeguarding personal information collected during intelligence activities. The section emphasises, "All persons should be treated with dignity and respect, regardless of their nationality or wherever they might reside, and all persons have legitimate privacy interests in the handling of their personal information". The White House, Presidential Policy Directive 28, 17 January 2014, p. 5.

bulk collection of data,[255] in what can be described as an echo of the findings of the CJEU in the 2014 *Digital Rights Ireland* case.[256] The U.S. Freedom Act was enacted on June 2 2015, imposing a series of limits on the bulk collection of telecommunication metadata on US citizens by US agencies such as the National Security Agency.

That notwithstanding, **the CJEU ruling *Digital Rights Ireland*** (Joined Cases C-293/12 and C-594/12) on data retention (section 3.2.2.3) **has much broader legal consequences** than merely the invalidation of the EU Data Retention Directive. The Court's reasoning is relevant across the board and the findings are also of particular significance when assessing the lawfulness of the various transatlantic agreements on data exchange and processing.

One of the key arguments used by the CJEU for annulling the Directive at issue was that the amount and precision of the data covered by this instrument allowed for very precise conclusions to be drawn concerning private lives: everyday habits, permanent and temporary residences, where people go, who they meet and places they visit; therefore generating a vague feeling in the public of constant surveillance.[257] The Court held that this allowed States to access all this information directly and this profoundly affected the private lives of everyone in the EU. It concluded that the system introduced by the Data Retention Directive constituted a particularly serious interference with the broader right of privacy enshrined in Article 7 EU Charter.

As the European Data Protection Supervisor (EDPS) stated in a Press Statement following the publication of the ruling by the Luxembourg Court,[258] "The judgment also means that the EU should take a firm position in discussions with third countries, particularly the US on the access and use of communications data of EU residents." Indeed, **remote unmediated access to electronic data under EU jurisdiction brings about further mistrust in wider EU-US relations**. How can the benchmarks developed by the CJEU in this ruling be respected in transatlantic relations in a context where access to data outside existing legal channels is proliferating?

---

[255] Privacy and Civil Liberties Oversight Board, Report on the Telephone Records Program Conducted Under section 215 of the U.S. Patriot Act and on the Operations of the Foreign Intelligence Surveillance Court (23 January 2014).

[256] See V. Mitsilegas (2015), "The Transformation of Privacy in an Era of Pre-emptive Surveillance", *Tilburg Law Review*, 20, pp. 35-57.

[257] The CJEU held, "[T]he fact that data are retained and subsequently used without the subscriber or registered user being informed is likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance", para. 37 of the judgment.

[258] Refer to https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/Press/2014/14-04-08_Press_statement_DRD_EN.pdf.

SECTION 5. WAYS FORWARD: SCENARIOS AND POLICY RECOMMENDATIONS

There are several scenarios when dealing with the legal and rule-of-law challenges inherent to third-country access to data for law enforcement and criminal justice purposes, in particular in the context of the EU-US MLA agreements. Three main options can be envisaged. They all share as a cross-cutting principle the prevalence of a mediated access model to data, which as examined in section 4 of this study is a pre-condition for fundamental rights and rule of law to be duly safeguarded.

5.1. Option 1. Enhancing the MLA agreement model

A first possibility would be to focus all efforts on ways to enhance existing legal provisions and procedures envisaged in the EU-US MLA framework within the current framework and without needing any general or specific legislative reform.

This option should take as a first step the establishment of an **objective and independent evaluation system** of the current practical implementation and operability of the transatlantic MLA system, which should be in turn subject to proper democratic and legal accountability. Such a system would accurately identify the main barriers and deficits characterising the EU-US MLA model. A key finding of this study is that such an evaluation or tracking method does not currently exist. There is not any publicly available statistical information on the frequency, quantitative uses and scope of MLA requests between the EU and the US.

This **'knowledge gap'** poses serious **obstacles for guaranteeing proper scrutiny and transparency** in a policy domain (judicial cooperation in criminal matters and police) where the EU is now sharing competence with EU Member States. It also increased the difficulty for conducting a 'consistency check' between EU Member States' bilateral MLA agreements and practices with the US on the gathering and exchange of evidence, and the model and common rules laid down in the EU-US MLA Agreement.

The result of such a system could lead to the elaboration by the European Commission and Eurojust, in close collaboration with the European Parliament, as well as relevant US authorities, of an **EU-US Guide for practitioners on the use and procedures in the EU-US MLA**. The focus of such a Guide would be in providing 'promising practices' to relevant national authorities for overcoming practical obstacles and ensuring some streamlining of procedures. Particular attention could be paid to the application and practical understandings of the main grounds for refusal of assistance in MLA requests envisaged by the Agreement, including questions of relevant national and European laws as well as the proportionality and fundamental rights tests. The ways in which

technologies and an online submission form could facilitate the daily operability of requests should be also explored.[259]

The EU Guide could also provide guidelines and common standards for ensuring **more transparency of the process and the clarity in the procedures**, including a uniform tracking system for the follow-up and update of the state of affairs and time-frame of EU-US MLA requests. Eurojust could also play a more active role in supporting and facilitating the execution of MLA requests between the EU and the US.[260] This should take place under close democratic scrutiny by the European Parliament, judicial control by the CJEU and relevant EU data protection bodies such as the European Data Protection Supervisor, Article 29 Working Party and the European Agency on Fundamental Rights (FRA).

Bilateral consultations and daily contacts between designated central authorities on both sides of the Atlantic has proved to be efficient when addressing and overcoming current obstacles affecting MLA processes. These should go hand-to-hand with **stronger political commitments by all the parties involved**, and corresponding judicial/law enforcement practices in line with those, on the usefulness and value of existing legal channels and MLA instruments for transatlantic cooperation in the gathering of and access to evidence.

Unmediated access to electronic data under foreign jurisdiction is not only an issue of USA authorities. EU Member States should refrain from similar

---

[259] The creation of an online submission form for MLAs was recommended by the U.S. President's Review Group Report "Liberty and Security in a Changing World: Report and Recommendations", 12 December 2013. The Report states that "[t]oday, there is no online form for foreign governments that seek to use the MLAT process. An online submission process, accompanied by clear information to foreign governments about the MLAT requirements, would make it easier for distant and diverse foreign governments to understand what is required under the US probable cause standard or other laws."

[260] This has been the case in a rather limited way in the past. This has included Eurojust requesting third States to speed up or facilitate the execution of extradition and MLA requests between Eurojust national desks and liaison prosecutors. Practical examples have included, e.g. execution of freezing and confiscation orders, hearings by videoconference, interception of communications, transfer of criminal proceedings, requests for criminal records, clarifying legal requirements and relevant legislation or identifying contact details of competent authorities. See Eurojust 2012 Annual Report (2013), Council 8179/13, 8 April 2013, which reads, "Eurojust's assistance was requested by the Italian authorities to facilitate the execution of MLA requests addressed to the competent authorities in the US and Portugal to acquire all the relevant information and documentation proving the fictitious nature of both subsidiaries. Thanks to Eurojust's speedy intervention, a quick response from the Portuguese authorities to the Italian MLA request was obtained, which resulted in the full payment of tax liabilities of the investigated Italian company within the time limits of the Italian preliminary investigation. The immediate reaction of Eurojust and the Portuguese authorities enabled the Italian authorities to recover EUR 67 million in unpaid taxes" (p. 56). See also Eurojust 2013 Annual Report (2014), p. 44. Eurojust provided assistance in 23 cases related to the US in 2013 and 18 in 2014. See a case illustration at http://eurojust.europa.eu/doclibrary/corporate/eurojust%20Annual%20Reports/Annual%20Report%202014/Annual-Report-2014-EN.pdf (p 47).

practices as they contravene EU law. Moreover, EU Member States and regional bodies (such as those in the context of the Council of Europe) should refrain from 'venue or forum shopping' practices seeking to amend, lower or renegotiate existing EU legal instruments and standards on mutual legal assistance and criminal justice cooperation. These are domains where the EU has exercised wide legal competence in recent decades and where clear and proper Union standards already exist, including (but not limited to) the EU-US MLA and the EIO.

RECOMMENDATIONS

5.1.1. The EU should set up an independent and objective evaluation system on the operability of EU-US MLA agreements, including statistical coverage of quantitative uses and frequency of use. An EU-US Guide for Practitioners on the Use and Procedures within the EU-US MLA Agreement should be adopted.

5.1.2. Eurojust could further facilitate cooperation between EU Member States and the US authorities in the execution of MLA requests, under close democratic scrutiny by the European Parliament, judicial control by the CJEU and relevant EU data protection bodies such as the European Data Protection Supervisor, Article 29 Working Party and the European Agency on Fundamental Rights (FRA).

5.1.3. All relevant Directorate Generals of the European Commission should more clearly express that current EU legal and rule-of-law standards on the gathering of data for law enforcement and criminal justice purposes should be fully respected and complied with in all open venues of cooperation with the US.

5.1.4. The Commission should also express concerns and block any further discussion on transborder access to data in the Council of Europe Cybercrime Committee (T-CY). Issues related to data protection, criminal justice and cybercrime fall now under EU competence and any international negotiations covering these matters fall under exclusive EU external competence, with the Commission now being in the driver's seat together with the European Parliament.

5.1.5. The European Parliament should reiterate its concerns on the T-CY's work and oppose any conclusion of an additional protocol to the Budapest Convention on Cybercrime which would legalise direct remote access to data held by private companies under EU jurisdiction.

5.1.6. Key priorities and pre-conditions for further cooperation should be the swift conclusion of the EU-US umbrella agreement (including the granting to EU citizens of protection in US jurisdiction), as well as the EU inter-institutional adoption of the data protection package.

5.2. Option 2. Improving the MLA agreement model – Legislative reform

A second option would entail revising the current EU-US MLA framework through legislative reforms. This scenario would focus on bringing the EU-US MLA agreement frameworks **in line with the EU post-Lisbon Treaty**

setting. As examined in this study, the set of EU legal instruments and standards have been profoundly reformed and fine-tuned since the entry into force of the Lisbon Treaty in December 2009.

The EU now has express legal competence concerning questions related to criminal justice and police cooperation, and ensures proper and timely enforcement of EU laws covering these domains in EU Member States. This has come with the official recognition of the European Parliament's role as 'co-legislator' in these areas.

A first key result of this new institutional setting has been the adoption of **the EIO, which provides benchmarks for future internal and external EU action in the domain of criminal justice**. These benchmarks include clear limits and parameters for the operation of mutual recognition in criminal matters between participating EU Member States. They cover, in particular, safeguards on the basis of domestic and constitutional provisions in the executing and issuing Member State, proportionality test and fundamental rights exceptions, in addition to the judicialisation of mutual legal assistance.

The EU-US MLA Agreement could be revised in order to closely align its current rules to post-Lisbon EU legal standards on criminal justice and privacy. This would entail reopening negotiations between the EU and the US on these issues. While there could be some risks in reopening the agreement and lowering existing standards, EU Member States are now duty-bound to comply with the benchmarks laid down in the EIO and the EU Charter of Fundamental Rights, including in their bilateral dealings with third countries or in regional venues such as the CoE.

If this option moves forward, the Union's responsibility would be to ensure that these standards function as the minimum foundations (red lines) for a new agreement to be concluded. Moreover, the EU should further ensure that all existing and future legal standards covering criminal justice cooperation are properly evaluated and codified in order **to ensure a consistent application of EU criminal law across the EU and strengthen the legitimacy (and prevent further fragmentation) of the common EU Justice Area**.

Any future legislative reform of the EU-US MLA model should not implement a 'mediator' system following a 'hybrid access to data model' similar to the one existing in the domain of European financial transactions with Europol. Eurojust should not be entrusted with a similar role, because this would pose fundamental accountability and transparency challenges with profound negative repercussions for the EU fundamental rights of the defence and to a fair trial.

RECOMMENDATIONS

5.2.1. The EU-US MLA model could be revised and amended in light of the EU post-Lisbon Treaty framework of legal standards and benchmarks in the domains of criminal justice and data protection.

5.2.2. The EIO provides a set of common legal benchmarks for EU internal and external action in the field of European criminal justice cooperation which could be used as the minimum criteria or red lines for any future revision of the EU-US MLA framework.

5.2.3. The European Commission and the European Parliament should better ensure consistent participation by all EU Member States in both enforcement and suspect rights measures in order to avoid incoherency and practical inoperability of the European Criminal Justice Area.

5.2.4. Eurojust should not become a 'mediator' allowing for a hybrid access to data model which would circumvent EU Member States centralised authorities' consent and independent review by relevant independent judicial authorities.

5.2.5. The EU should call for the consolidation and even codification of existing EU rules and instruments dealing with judicial cooperation in criminal matters, which could lead to the adoption of a Common Corpus of European Criminal Law laying down all EU legal standards in criminal justice cooperation, including those in cooperation with third countries.[261] This should go hand-to-hand with an effective and independent evaluation mechanism on the functioning of the EU criminal justice cooperation.[262]

5.3. Option 3: Towards a transatlantic investigation order – Mutual recognition across the Atlantic?

A third and by far more ambitious long-term scenario would be the development of a **common justice area across the Atlantic**. This would entail transferring and exporting the EU principle of mutual recognition in criminal justice cooperation in the Union's relation with the US. Such a model should aim at ensuring a reinvigorated and revamped system of

[261] As proposed in V. Mitsilegas et al. (2014), "The End of the Transitional Period for Police and Criminal Justice Measures Adopted before the Lisbon Treaty: Who Monitors Trust in the European Justice Area?", CEPS Liberty and Security in Europe Series, Centre for European Policy Studies, Brussels.

[262] See Article 70 of the TFEU, which reads, "[T]he Council may, on a proposal from the European Commission, adopt measures laying down the arrangements whereby Member States, in collaboration with the Commission, conduct objective and independent evaluation of the implementation of Union policies…in particular in order to facilitate the application of the principle of mutual recognition". Refer to the European Parliament Resolution of 27 February 2014 with recommendations to the Commission on the review of the European Arrest Warrant (2013/2109(INL)).

cooperation for the purposes of law enforcement in the context of criminal justice investigations.

This scenario would lead to the adoption of a **Transatlantic Investigation Order (TIO) system** seeking primarily to speed up and make more efficient cooperation between US and EU authorities in the field of criminal justice. The TIO would take the 'benchmarks' currently existing in the EIO as the core basis for cooperation. A system of such a nature would require close judicial scrutiny by the Court of Justice of the EU.

It would also institutionalise **EU-US mutual trust, while formalising the scope and use of grounds for refusing** to give data to a requesting State. These would include the application of exceptions on grounds of proportionality, fundamental rights and legality tests. This should go hand-to-hand with submitting the TIO system to existing EU legal standards on privacy and criminal justice procedural rights of suspects.

RECOMMENDATION

5.3.1. The EU and the US could in the future explore the possibility of establishing mutual recognition of judicial decisions in criminal justice which have been issued/validated by an independent judicial authority to gather evidence in a State party. The EIO could be used as a model for a Transatlantic Investigation Order (TIO).

REFERENCES

Aalto, P. et al. (2014), "Article 47 – Right to an Effective Remedy and to a Fair Trial", in S. Peers, T. Hervey, J. Kenner and A. Ward (eds), *The EU Charter of Fundamental Rights: A Commentary*, Oxford: Hart Publishing.

Alldridge, P. (2012), "UK Bribery Act: The Caffeinated Younger Sibling of the FCPA", *Ohio St. LJ* 73 (2012): 1181.

Amicelle, A. (2011), "The Great (Data) Bank Robbery: Terrorist Finance Tracking Program and the 'SWIFT Affair'", Research Question 36, CERI, Sciences-Po, Paris.

Bigo, D. et al. (2013), "Mass Surveillance of Personal Data by EU Member States and its compatibility with EU Law", CEPS Liberty and Security Series, Centre for European Policy Studies, Brussels.

Bigo, D. et al. (2014), "National Security and Secret Evidence in Legislation and Before the Courts: Exploring the Challenges", CEPS Liberty and Security in Europe Series, Centre for European Policy Studies, Brussels.

Bigo, D. et al. (2011), "Towards a New EU Legal Framework for Data Protection and Privacy: Challenges, Principles and the Role of the European Parliament" (Policy Department C on Citizens' Rights and Constitutional Affairs of the Directorate General for Internal Policies of the European Parliament), especially pp. 74-78.

Binns, R. D., D. Millard and L. Harris (2014), "Data havens, or privacy sans frontières?: a study of international personal data transfers", *Proceedings of the 2014 ACM conference on Web science*, ACM.

Brouwer, E. (2008), *Digital Borders and Real Rights: Effective Remedies for Third-Country Nationals in the Schengen Information System*, Leiden: Martinus Nijhoff Publishers, especially pp. 155-176.

Carrera, S. and F. Geyer (2008), "The Reform Treaty and Justice and Home Affairs – Implications for the common Area of Freedom, Security and Justice', in E. Guild and F. Geyer (eds), *Security versus Justice? Police and Judicial Cooperation in the European Union*, Aldershot: Ashgate Publishing, pp. 289-307.

Carrera, S. et al. (2013), "Europe's Most Wanted? Recalibrating Trust in the European Arrest Warrant System", CEPS Liberty and Security in Europe Series, Centre for European Policy Studies, Brussels.

Colangelo, A. J. (2014), "What is Extraterritorial Jurisdiction?", *Cornell Law Review*.

Costello, C. (2006), "The Bosphorus ruling of the European Court of Human Rights: Fundamental rights and blurred boundaries in Europe", *Human Rights Law Review* 6.1: 87-130.

De Búrca, G. (2013), "After the EU Charter of Fundamental Rights: The Court of Justice as a Human Rights Adjudicator? ", *Maastricht Journal of European and Comparative Law* 20, no. 2: 168-84.

González Fuster, G. (2014), *The Emergence of Personal Data Protection as a Fundamental Right of the EU,* Dordrecht: Springer.

González Fuster, G. and S. Gutwirth (2013), "Opening up Personal Data Protection: A Conceptual Controversy," *Computer Law & Security Review* 29: 531-39.

González Fuster, G., P. De Hert and S. Gutwirth (2008), "SWIFT and the vulnerability of transatlantic data transfers", *International Review of Law, Computers & Technology*, Vol. 22, No. 1: 191-202.

Guild, E. and S. Carrera (2014), "The Political and Judicial Life of Metadata: Digital Rights Ireland and the Trail of the Data Retention Directive", CEPS Liberty and Security in Europe Series, Centre for European Policy Studies, Brussels.

Hijmans, H. and A. Scirocco (2009), "Shortcomings in EU Data Protection in the Third and the Second Pillars: Can the Lisbon Treaty Be Expected to Help?", *Common Market Law Review* 46: 1485-1525.

Kokott, J. and C. Sobotta (2013), "The distinction between privacy and data protection in the jurisprudence of the CJEU and the EctHR", *International Data Privacy Law*, Vol. 3, No. 4: 222-228.

Korff, D. (2014), "The Rule of Law on the Internet and in the Wider Digital World", Issue Paper Published by the Council of Europe Commissioner for Human Rights, Council of Europe.

Lynskey, O. (2014), "Deconstructing Data Protection: The 'Added Value' of a Right to Data Protection in the EU Legal Order", *International and Comparative Law Quarterly*, Vol. 63, Issue 3: 569-597.

Markus Funk, T. (2014), "Mutual Legal Assistance Treaties and Letters Rogatory: A Guide for Judges", Federal Judicial Centre, International Litigation Guide, pp. 1 and 23.

Mitsilegas, V. (2003), "The New EU-US Co-operation on Extradition, Mutual Legal Assistance and the Exchange of Police Data", *European Foreign Affairs Review*, Vol. 8: 515-536.

Mitsilegas, V. (2006), "The Constitutional Implications of Mutual Recognition in Criminal Matters in the EU", *Common Market Law Review*, Vol. 43: 1277-1311.

Mitsilegas, V. (2009), *EU Criminal Law*, Oxford: Hart Publishing.

Mitsilegas, V. (2012), "The Limits of Mutual Trust in Europe's Area of Freedom, Security and Justice. From Automatic Inter-state Cooperation to the Slow Emergence of the Individual", *Yearbook of European Law 2012*, Vol. 31: 319-372.

Mitsilegas, V. (2012), "The Area of Freedom, Security and Justice from Amsterdam to Lisbon. Challenges of Implementation, Constitutionality and Fundamental Rights", General Report, in J. Laffranque (ed.), The Area of Freedom, Security and Justice, Including Information Society Issues, Reports of the XXV FIDE Congress, Tallinn, Vol. 3, pp. 21-142.

Mitsilegas, V. (2014), "Transatlantic counterterrorism cooperation and European values: The elusive quest for coherence", in E. Fahey and D. Curtin (eds), *A Transatlantic Community of Law*, Cambridge: Cambridge University Press, pp. 289-315.

Mitsilegas, V. (2015), "The Transformation of Privacy in an Era of Pre-emptive Surveillance", *Tilburg Law Review*, 20: 35-57.

Mitsilegas, V. (forthcoming), "Managing Legal Diversity in Europe's Area of Criminal Justice: The Role of Autonomous Concepts", in R. Colson and S. Field (eds), *EU Criminal Justice and the Challenges of Legal Diversity. Towards A Socio-Legal Approach to EU Criminal Policy,* Cambridge: Cambridge University Press.

Mitsilegas, V. et al. (2014), "The End of the Transitional Period for Police and Criminal Justice Measures Adopted before the Lisbon Treaty: Who Monitors Trust in the European Justice Area?", CEPS Liberty and Security in Europe Series, Centre for European Policy Studies, Brussels.

O'Neill, M. (2010), "The Issue of Data Protection and Data Security in the (Pre-Lisbon) EU Third Pillar", *Journal of Contemporary European Research*, Vol. 6, No. 2: 211-235.

Peers, S., T. Hervey, J. Kenner and A. Ward (eds) (2014), *The EU Charter of Fundamental Rights: A Commentary*, Oxford: Hart Publishing.

Reydams, L. (2000), "Universal Criminal Jurisdiction: The Belgian State of Affairs", *Criminal Law Forum*, Vol. 11. No. 2.

Roach, K. (2010), "The Eroding Distinction Between Intelligence and Evidence in Terrorism Investigations", in N. McGarrity, A. Lynch and G. Williams (eds), *Counter-Terrorism and Beyond*, London: Routledge, pp. 48-68.

Woods, A.K. (2015), "Data beyond Borders: Mutual Legal Assistance in the Internet Age", Global Network Initiative.

ABBREVIATIONS

AFSJ	Area of Freedom, Security and Justice
AG	Advocate General
CoE	Council of Europe
COM	European Commission
CJEU	Court of Justice of the European Union
EAW	European Arrest Warrant
ECHR	European Convention on Human Rights (1950)
ECtHR	European Court of Human Rights
EP	European Parliament
EU	European Union
EU-US MLA	EU-US Agreement on Mutual Legal Assistance
EUCFR	Charter of Fundamental Rights of the European Union
EUMS	European Union Member State(s)
EUROJUST	The European Union's Judicial Cooperation Unit
EIO	European Investigation Order
FISA	Foreign Intelligence Surveillance Act
JHA	Justice and Home Affairs
LIBE	European Parliament Committee on Civil Liberties, Justice and Home Affairs
MLA	Mutual Legal Assistance
MLAT	Mutual Legal Assistance Treaty
MEP	Member of the European Parliament
NSA	National Security Agency (US)
PNR	Passenger Name Records
SCA	Stored Communications Act
SWIFT	Society for Worldwide Interbank Financial Telecommunication
T-CY	Cybercrime Convention Committee
TFTP	Terrorist Finance Tracking Program
US	United States

ABOUT THE AUTHORS

Dr Sergio Carrera is Senior Research Fellow and Head of the Justice and Home Affairs section at the Centre for European Policy Studies (CEPS) and Associate Professor at the Faculty of Law of the University of Maastricht.

Dr Gloria González Fuster is a Research Professor at the Vrije Universiteit Brussel (VUB).

Prof. Elspeth Guild is Senior Associate Research Fellow at the Centre for European Policy Studies (CEPS), Brussels. She is Jean Monnet Professor ad personam of European immigration law at Radboud University Nijmegen as well as Queen Mary University of London.

Prof. Valsamis Mitsilegas is Head of the Department of Law and Professor of European Criminal Law at Queen Mary University of London.

This study examines the challenges to European law posed by third-country access to data held by private companies for purposes of law-enforcement investigations in criminal proceedings. The proliferation of electronic communications is putting cloud-computing companies under severe strain from multiple demands from the authorities to acquire access to such data.

A key challenge for the EU emerges when third-country authorities request access to data held by private companies under EU jurisdiction outside pre-established channels of cooperation, in particular outside Mutual Legal Assistance (MLA) treaties. The EU concluded an MLA agreement with the United States in 2003, which sets out the rules and procedures for lawful and legitimate access to evidence. A key distinguishing feature of the MLA-led process is that any request for access to data is 'mediated' by or requires the consent of the state authority to whom the request is submitted as well as scrutiny by an independent judicial authority.

Special focus is given in this study to the practical issues emerging in EU-US relations covering mutual legal assistance and evidence-gathering for law enforcement purposes in criminal proceedings. The fundamental question guiding this enquiry is: How best to ensure that the rule of law and trust-based methods are respected in these proceedings?

In conducting this study, the authors carried out a detailed survey of the main EU legal instruments and their standards, underlining their direct relevance for assessing the lawfulness and legitimacy of access to data. They then outline three possible scenarios for the future and put forward a set of policy recommendations for addressing these challenges.

Centre for European Policy Studies
1 Place du Congrès
1000 Brussels, Belgium
Tel: 32(0)2.229.39.11
Fax: 32(0)2.219.41.51
E-mail: info@ceps.eu
Website: www.ceps.eu

9 789461 384683

CENTRE FOR EUROPEAN POLICY STUDIES